Technická univerzita v Liberci

FAKULTA PŘÍRODOVĚDNĚ-HUMANITNÍ A PEDAGOGICKÁ

Katedra: Katedra matematiky a didaktiky matematiky

Studijní program: B1101 Matematika

Studijní obor: Matematika

EUKLIDŮV ALGORITMUS V MINULOSTI A SOUČASNOSTI

EUCLIDEAN ALGORITHM IN THE PAST AND THE PRESENT

Bakalářská práce: 13–FP–KMD–001

Autor:
Hana HOFFMANOVÁ

Podpis:

.....

Vedoucí práce: doc. RNDr. Jaroslav Vild

Konzultant:

Počet

stran	grafů	obrázků	tabulek	pramenů	příloh
58	0	0	10	24	4

V Liberci dne: 22. 4. 2013

TECHNICKÁ UNIVERZITA V LIBERCI
Fakulta přírodovědně-humanitní a pedagogická
Akademický rok: 2011/2012

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Hana Hoffmanová**
Osobní číslo:	**P10000003**
Studijní program:	**B1101 Matematika**
Studijní obor:	**Matematika**
Název tématu:	**Euklidův algoritmus v minulosti a současnosti**
Zadávající katedra:	**Katedra matematiky a didaktiky matematiky**

Zásady pro vypracování:

Cíle práce:
- vypracování přehledu o Euklidově algoritmu, popis jeho využití
- doporučení pro uživatele Euklidova algoritmu
- prezentace práce

Požadavky na zpracování:
- zpracování konceptu, jehož východiskem jsou doporučené a nalezené prameny
- sběr, analýza a interpretace získaných informací
- zpracování podrobné struktury textu a prezentace
- konzultace s vedoucím práce
- splnění současných pravidel pro bibliografické citace a ČSN normy

Metody:
- studium literatury a jiných informačních zdrojů

Rozsah grafických prací:

Rozsah pracovní zprávy:

Forma zpracování bakalářské práce: **tištěná/elektronická**

Seznam odborné literatury:

Lauritzen, N. Concrete Abstract Algebra. Cambridge, University Press, 2006.
Mollin, R.A. Fundamental Number Theory with Applications. 2nd edit. Chapman and Hall, 2008.
Knuth, D.E. Umění programování, 1.díl Základní algoritmy.Computer Press, 2008.
Scheid, H. Elemente der Arithmetik und Algebra. 2. Afg. Wissenschaftsverlag, Mannheim, 1992. ISBN 3-411-14922-1.
http://en.wikipedia.org/wiki/Euclidean_algorithm

Vedoucí bakalářské práce: **doc. RNDr. Jaroslav Vild**
Katedra matematiky a didaktiky matematiky

Datum zadání bakalářské práce: **17. dubna 2012**
Termín odevzdání bakalářské práce: **26. dubna 2013**

doc. RNDr. Miroslav Brzezina, CSc.
děkan

L.S.

doc. RNDr. Jaroslav Mlýnek, CSc.
vedoucí katedry

dne

Čestné prohlášení

Název práce:	Euklidův algoritmus v minulosti a současnosti
Jméno a příjmení autora:	Hana Hoffmanová
Osobní číslo:	P10000003

Byla jsem seznámena s tím, že na mou bakalářskou práci se plně vztahuje zákon č. 121/2000 Sb. o právu autorském, právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon), ve znění pozdějších předpisů, zejména § 60 – školní dílo.

Prohlašuji, že má bakalářská práce je ve smyslu autorského zákona výhradně mým autorským dílem.

Beru na vědomí, že Technická univerzita v Liberci (TUL) nezasahuje do mých autorských práv užitím mé bakalářské práce pro vnitřní potřebu TUL.

Užiji-li bakalářskou práci nebo poskytnu-li licenci k jejímu využití, jsem si vědom povinnosti informovat o této skutečnosti TUL; v tomto případě má TUL právo ode mne požadovat úhradu nákladů, které vynaložila na vytvoření díla, až do jejich skutečné výše.

Bakalářskou práci jsem vypracovala samostatně s použitím uvedené literatury a na základě konzultací s vedoucím bakalářské práce a konzultantem.

Prohlašuji, že jsem do informačního systému STAG vložila elektronickou verzi mé bakalářské práce, která je identická s tištěnou verzí předkládanou k obhajobě a uvedla jsem všechny systémem požadované informace pravdivě.

V Liberci dne: 22. 04. 2013

.....

Hana Hoffmanová

Poděkování

Děkuji vedoucímu bakalářské práce doc. RNDr. Jaroslavu Vildovi za vstřícný přístup, cenné rady, připomínky a metodické vedení práce.

Abstrakt

Tato bakalářská práce se zabývá Euklidovým algoritmem a pojmy, které s ním souvisí. Práce se skládá z devíti kapitol, v každé je popsána teorie k danému problému a uveden minimálně jeden příklad. Některé kapitoly jsou doplněny o historickou poznámku. Cílem práce je poskytnout přehled o Euklidově algoritmu, jaký je jeho význam, jak a kde se dá využít a co je s ním spojené.

Klíčová slova: Euklidův algoritmus, největší společný dělitel, rozšířený Euklidův algoritmus, Bézoutova rovnost, kongruence, inverzní prvek, řetězové zlomky, polynomy.

Abstract

This thesis deals with the Euclidean algorithm and terms associated with it. The work consists of nine chapters, each one describes the theory of a given problem and gives at least one example. Some chapters are supplemented by a historical note. The aim of thesis is to provide an overview of Euclidean algorithm, what is its meaning, how and where can be used it, and what is associated with it.

Key words: Euclidean algorithm, the greatest common divisor, extended Euclidean algorithm, Bézout's identity, kongruence, inverse, continued fractions, polynomials.

Obsah

Použité matematické značky a symboly

$\mathbb{N}$	množina všech přirozených čísel
$\mathbb{Z}$	množina všech celých čísel
$\mathbb{R}$	množina všech reálných čísel
$\mathbb{Z}_m$	množina zbytkových tříd modulo m
$\mathbb{Z}_p$	množina zbytkových tříd modulo p ($p$rvočíslo)
T	těleso
$a \in \mathrm{A}$	a je prvkem množiny A
… := …	… je definováno jako …
NSD	největší společný dělitel
NSD(a, b)	největší společný dělitel čísel a, b
$a \mid b$	a dělí b beze zbytku; $a, b \in \mathbb{Z}$
b^{-1}	inverzní prvek k b (modulo)
$a \equiv_m b,\ a \equiv b \pmod{m}$	a je kongruentní s b modulo m
$f(x)$	polynom
st(f)	stupeň polynomu $f(x)$
$\varphi(n)$	Eulerova funkce
ϕ	zlatý řez
$\lfloor x \rfloor$	dolní celá část čísla x
$\lceil x \rceil$	horní celá část čísla x
$\log_a b$	logaritmus o základu a čísla b
F_n	n-té Fibonacciho číslo

Úvod

Tématem bakalářské práce je Euklidův algoritmus. Podle mého názoru je tento pojem širší veřejnosti neznámý, kdykoli se mě někdo zeptal, o čem píši bakalářskou práci, a já odpověděla, že o Euklidově algoritmu, jen málo lidí vědělo, co to znamená. Ve chvíli, kdy člověk znal tento pojem, tušil pouze, že má spojení s největším společným dělitelem. Volba tématu byla pro mě po jednoduché úvaze celkem snadná. Žádné z nabízených témat mě tolik neoslovilo, a proto jsem začala přemýšlet o vlastním. Protože je mi bližší algebra než analýza, bylo jasné, z jaké oblasti vybírat. Po delším hledání mi přišel sympatický Euklidův algoritmus, když jsem si o něm zjistila více, bylo vybráno.

V následujícím textu se pokusím vysvětlit, kde se dá Euklidův algoritmus použít a jak. Euklidův algoritmus se nepoužívá jen k určení největšího společného dělitele dvou přirozených čísel, jak to popisuje Euklid sám, ale má spoustu modifikací, rozšíření a užitečné využití. Cílem práce je, aby posloužila všem, kteří se chtějí o Euklidově algoritmu něco dozvědět, měl by to být takový průvodce obsahující základní pojmy související s Euklidovým algoritmem a možnostmi použití. Pokusila jsem se o vytvoření uceleného textu, který obsahuje podstatné základy nauky o Euklidově algoritmu. V každé kapitole se snažím uvést teorii a k tomu alespoň jeden praktický příklad, protože se domnívám, že jeden pořádný příklad objasní danou látku mnohem lépe a rychleji než několik stránek složených pouze z vět, definic a důkazů. Protože bakalářská práce nese název *Euklidův algoritmus v minulosti a současnosti*, přidala jsem k některým kapitolám zajímavosti z historie matematiky. Některé historické poznámky nesouvisí přímo s Euklidovým algoritmem, ale s jiným pojmem obsaženým v dané kapitole.

V první kapitole je Euklidův algoritmus uveden v původní podobě pro představu, jaká byla jeho prvotní formulace. Euklidův algoritmus se primárně používá k nalezení nevětšího společného dělitele dvou čísel, to uvádí druhá kapitola. S největším společným dělitelem úzce souvisí jeho vyjádření jako lineární kombinace vstupních čísel, která se nazývá Bézoutova rovnost, o té hovoří třetí kapitola. Zde se k pojmu Euklidův algoritmus připojuje přívlastek rozšířený,

neboť vedle NSD nalézá též lineární kombinaci. Další kapitola představí modulární aritmetiku, v níž jsou často potřebné inverzní prvky. Na konci této kapitoly je zmínka o šifrovacím algoritmu RSA, který se využívá k zabezpečení informací. Euklidův algoritmus je součástí šifrovacího procesu. Kapitola pátá ukazuje, že se Euklidův algoritmus dá použít nejen pro přirozená čísla, ale i pro další obory, jako jsou racionální čísla nebo polynomy, o kterých se hovoří v následující šesté kapitole. Obory, kde je zajištěna funkčnost Euklidova algoritmu se nazývají Euklidovské obory. Euklidův algoritmus souvisí také s čínskou zbytkovou větou, kterou přiblíží kapitola sedmá. Zde jsou uvedeny zajímavé příklady, které využívají právě čínskou větu o zbytcích. Osmá kapitola pojednává o souvislosti Euklidova algoritmu s Fibonacciho čísly, ta jsou velmi zajímavá, mají pozoruhodné vlastnosti a dala by se o nich napsat samostatná práce. Poslední kapitola předvádí dnešní podobu Euklidova algoritmu, a to v počítačové formě, přesněji zapsanou v programovacím jazyku. Tak jako první kapitola uvádí původní formulaci Euklidova algoritmu, tak poslední kapitola uzavírá práci ukázkou počítačové verze.

Při tvorbě bakalářské práce jsem postupovala od prvního seznámení s vybraným tématem přes shromažďování zdrojů a literatury až k zapisování sesbíraných informací a uspořádání celé práce. Nasbírané údaje z různých zdrojů jsem porovnala, zjistila, v čem se liší, a vybrala ty nejvhodnější. Většinu příkladů jsem vytvořila sama, jednak pro originalitu a jednak pro vlastní kontrolu, zda vše platí, jak je uváděno. Používáním tabulek pro zápis Euklidova algoritmu jsem se inspirovala v přednáškách doc. RNDr. Jaroslava Vilda. Myslím, že jsou velmi užitečné a mnohem přehlednější než vypisování jednotlivých kroků pod sebe. Je škoda, že jsou v odborné literatuře tak málo využívány.

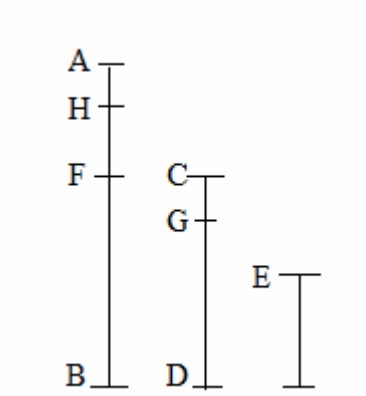
Doufám, že si každý čtenář najde v této bakalářské práci něco nového či zajímavého, nebo alespoň nahlédne na Euklidův algoritmus z jiného pohledu.

1 Původní Euklidův algoritmus

Euklides popsal tento algoritmus v díle *Základy*, v Knize VII, kde algoritmus popisují první tři tvrzení. Níže jsem přepsala první dvě tvrzení z Knihy sedmé, každé ve dvou podobách, kde starší znění je český překlad kritického vydání Heiberga (1883) napsaný roku 1907 Františkem Servítem, novější podoba je přepracované znění od Petra Vopěnky, které je srozumitelnější. Starší verze je psána archaickou češtinou, což může zpočátku způsobovat nedorozumění, například výraz *číslo kmenné* znamená prvočíslo nebo *čísla navzájem kmenná* jsou čísla nesoudělná. Také jsou zde přirozená čísla znázorněna délkami úseček označenými jejich koncovými body, což může být náročnější na představu. První tvrzení popisuje, kdy jsou dvě čísla nesoudělná. Jsou-li soudělná, lze nalézt jejich největšího společného dělitele, což říká druhé tvrzení. Třetí tvrzení Knihy sedmé je rozšířením druhého tvrzení na tři čísla, tedy popsané pro největšího společného dělitele tří čísel.

PRVNÍ TVRZENÍ

„**I. Jsou-li dána dvě čísla nestejná a odčítá-li se střídavě vždy menší od většího, když zbývající předcházejícího nikdy nedoměřuje, dokud nezbude jednotka, počáteční čísla budou navzájem kmenná.**



Nuže ze dvou čísel *AB*, *CD*, odčítá-li se střídavě vždy menší od většího, zbývající nikdy nedoměřuj předcházejícího, dokud nezbude jednotka; pravím, že *AB*, *CD* jsou navzájem čísla kmenná, tj. že *AB*, *CD* doměřuje jednotka jediná.

Neboť nejsou-li *AB*, *CD* čísla navzájem kmenná, bude je měřiti nějaké číslo. Měř je a buď to *E*; a *CD* měříc *BF* ostavuj menší sebe *FA*, *AF* pak měříc *DG* ostavuj menší sebe *GC* a *GC* měříc *FH* ostavuj jednotku *HA*.

Ježto tedy *E* měří *CD*, *CD* pak měří *BF*, tedy též *E* měří *BF*; měří však též celou veličinu *BA*; tedy též zbytek *AF* bude měřiti. *AF* pak měří *DG*; tedy též *E* měří veličinu *DG*; jest však měrou i celému *DC*; tedy též zbytku *CG* bude měrou. *CG*

však měří *FH*; tedy též *E* bude měřiti veličinu *FH*; jest však měrou též celému *FA*, tedy též zbývající jednotce *AH* bude měrou, ač je číslem; což právě nemožno. Tedy čísel *AB*; *CD* nebude měřiti žádné číslo; pročež *AB*, *CD* jsou čísla navzájem kmenná.“ [4 s. 103]

„**I. Nechť čísla *a*, *b* jsou dělitelná číslem *d*. Potom platí:**

1) Číslo *a* + *b* je dělitelné číslem *d*.

2) Je-li *b* < *a*, pak číslo *a* – *b* je dělitelné číslem *d*.

Protože je $a = a' \times d$, $b = b' \times d$, je $a + b = (a' + b') \times d$. Je-li $b < a$, je i $b' < a'$, a tedy $a - b = (a' - b') \times d$.

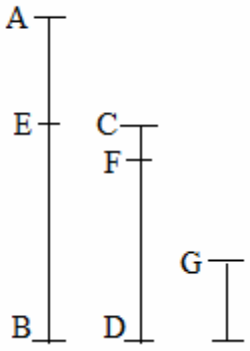
Důsledek. Jestliže v průběhu Eukleidova algoritmu použitého na nějakou danou dvojici čísel vznikne dvojice čísel, jejichž společným dělitelem je číslo *d*, pak číslo *d* je společným dělitelem každé dvojice čísel, která v průběhu tohoto algoritmu vznikne (tudíž i dvojice výchozí, i dvojice cílové).“ [4 s. 53]

DRUHÉ TVRZENÍ

„**II. Jsou-li dána dvě čísla navzájem nekmenná, najdi největší jejich společnou míru.**

Danými dvěma čísly navzájem nekmennými buďtež *AB*, *CD*; má se tedy nalézti čísel *AB*, *CD* největší společná míra.

Jestliže ovšem *CD* měří veličinu *AB* a je též samo sobě měrou, tedy *CD* je společnou měrou čísel *CD*, *AB*, i zřejmo, že též největší, neboť žádné nad *CD* větší nebude čísla *CD* měřiti.



Pakli *CD* neměří čísla *AB*, budeme-li z čísel *AB*, *CD* střídavě vždy menší od většího odčítati, zbude nějaké číslo, jež bude měrou předcházejícího. Jednotka zajisté nezbude, sice budou *AB*, *CD* navzájem kmennými, což však proti podmínce. Tedy zbude nějaké číslo, jež bude měrou

předcházejícího. I ostavuj *CD* měříc *BE* menší sebe *EA*, *EA* pak měříc *DF* ostavuj menší sebe *FC*, *CF* pak *AE* doměřuj. Ježto tedy *CF* měří *AE*, *AE* pak měří *DF*, tedy *CF* bude měřiti *DF*; měří však i sebe, tedy též celému *CD* bude měrou. *CD* však měří *BE*, tedy též *CF* měří veličinu *BE*; měří však též *EA*, protož i celému *BA* bude měrou; měří však též *CD*; *CF* tedy měří čísla *AB*, *CD*. Pročež *CF* je společnou mírou čísel *AB*, *CD*.

Pravím ovšem, že též největší. Neboť není-li *CF* největší společnou měrou čísel *AB*, *CD*, bude čísla *AB*, *CD* měřiti číslo větší než *CF*. Měř je a buď jím *G*. A ježto *G* měří *CD*, *CD* pak měří *BE*, tedy též *G* měří *BE*; jest však i celému *BA* měrou, tedy též zbytku *AE* bude měrou. *AE* však měří *DF*, pročež i *G* bude měřiti *DF*; však i celému *DC* měrou, tedy též zbytku *CF* bude měrou, větší menšímu, což právě nemožno. Tedy číslům *AB*, *CD* nebude měrou žádné číslo větší než *CF*; pročež *CF* je největší společnou měrou čísel *AB*, *CD*.

Důsledek. Z toho zajisté patrno, že když číslo dvě čísla doměřuje, též největší společnou míru jejich bude doměřovati.“ [4 s. 104–105]

„**II. Cílové číslo *d* Eukleidova algoritmu použitého na dvojici čísel *a*, *b* je největším společným dělitelem čísel *a*, *b*.**

Protože číslo *d* je dělitelem čísel z cílové dvojice *d*, *d*, je podle důsledku tvrzení I též dělitelem čísel *a*, *b*. Je-li *e* dělitelem čísel *a*, *b*, je podle důsledku tvrzení I číslo *e* dělitelem čísel náležících do cílové dvojice *d*, *d*. Odtud $e \leq d$.

Důsledky:

1) Každý společný dělitel čísel *a*, *b* je dělitelem největšího společného dělitele čísel *a*, *b*.

2) Čísla *a*, *b* jsou nesoudělná právě tehdy, když číslo 1 je cílovým číslem Eukleidova algoritmu použitého na dvojici čísel *a*, *b*.“ [4 s. 53–54]

2 Euklidův algoritmus – Největší společný dělitel

Nejrozšířenějším, a také asi nejznámějším použitím Euklidova algoritmu, je hledání největšího společného dělitele dvou přirozených čísel. *Největší společný dělitel* dvou přirozených čísel je největší číslo takové, jímž jsou obě čísla dělitelná neboli je vydělí beze zbytku.

Platí: 1) NSD(0, 0) := 0 definice NSD

2) NSD(a, a) = a idempotence

3) NSD(a, b) = NSD(b, a) komutativita

4) NSD(a, b) = NSD(a, $b - a$), $b > a$

K označení největšího společného dělitele se používá NSD, NSD(a, b), Nsd(a, b) nebo jednodušeji (a, b). V anglickém jazyce se používá označení gcd(a, b), což je zkratkou termínu *greatest common divisor*.

Největšího společného dělitele můžeme získat kanonickým rozkladem čísel a, b na mocniny prvočísel. Například pro nalezení NSD(24, 20) uděláme rozklad na prvočísla

$$24 = 2 \cdot 2 \cdot 2 \cdot 3 = 2^3 \cdot 3^1$$
$$20 = 2 \cdot 2 \cdot 5 = 2^2 \cdot 5$$

a z nich vezmeme nejmenší společné mocniny prvočísel. Největší společný dělitel čísel 24 a 20 bude tedy 4, protože

$$\text{NSD}(24, 20) = 2^{\min\{3,2\}} \cdot 3^{\min\{1,0\}} \cdot 5^{\min\{0,1\}} = 4.$$

Pro velká čísla je však obtížné nalézt rozklad na mocniny prvočísel, proto se používá metoda zvaná *Euklidův algoritmus*, která efektivně nalezne největšího společného dělitele i bez rozkládání na prvočinitele, a to pomocí dělení se zbytkem.

Věta 2.1 (O dělení se zbytkem) Nechť pro všechna $a \in \mathbb{Z}$, $b \in \mathbb{N}$, $b \neq 0$, potom existuje jediné q, $r \in \mathbb{Z}$ taková, že $a = bq + r$, kde $0 \leq r < b$.

Euklidův algoritmus spočívá v opakování konečně mnoha kroků, kdy máme na začátku čísla a, b a nejdříve najdeme jejich zbytek po dělení a/b, který označíme

r_0. Poté posuneme dělení na b/r_0 a získáme zbytek r_1. Pak vezmeme r_0/r_1 a dostaneme zbytek r_2. Takto postupujeme až do té doby, dokud není dělitel nulový. NSD je pak poslední nenulový zbytek. Pro zápis algoritmu můžeme použít i tabulku, kam zapisujeme zbytky po dělení r_j a podíly q_j.

2.1 Popis Euklidova algoritmu

Mějme dvě přirozená čísla a a b a hledáme jejich NSD(a, b), nechť $a > b$, položme $a = r_{-1}$, $b = r_0$, takže

$$r_{-1} = q_1 r_0 + r_1,$$

kdyby $r_1 = 0$, pak b dělí a a NSD(a, b) = b. Jestliže $r_1 \neq 0$, pak Euklidův algoritmus pokračuje dál:

$$\begin{aligned} r_0 &= q_2 r_1 + r_2 \\ &\vdots \\ r_{n-2} &= q_n r_{n-1} + \boldsymbol{r_n} \\ r_{n-1} &= q_{n+1} r_n + 0, \qquad r_n \neq 0 \end{aligned}$$

r_n je poslední nenulový zbytek a je roven NSD(a, b).

Tvrzení 2.2 Jestliže je NSD = 1, pak jsou čísla a, b nesoudělná.

> 1, pak jsou čísla soudělná.

Pro větší přehlednost je dobré použít tabulku:

j	-1	0	1	2	…	n	$n+1$
$r_{j-2} - q_j \cdot r_{j-1} =: r_j$	a	b	r_1	r_2	…	r_n	r_{n+1}
q_j			q_1	q_2	…	q_n	q_{n+1}

Lemma 2.3 Jestliže $a = q \cdot b + r$, pak NSD(a, b) = NSD(b, r), tedy největší společný dělitel dělence a a dělitele b se rovná největšímu společnému děliteli zbytku po dělení r a děliteli b.

Důkaz: Nechť d = NSD(a, b), pak vztahy $d \mid a$ a $d \mid b$ dohromady naznačují, že $d \mid (a - q \cdot b)$ nebo $d \mid r$. Tedy d je společný dělitel b i r. Na druhé straně, jestliže

c je libovolný společný dělitel b a r, pak $c \mid (q \cdot b + r)$, odkud $c \mid a$. To dělá c společným dělitelem a a b, tak že $c \leq d$. Z definice NSD(b, r) teď plyne, že d = NSD(b, r). [2 s. 26–27] □

Tvrzení 2.4 Jestliže $a \mid bc$, a a b jsou nesoudělné, pak $a \mid c$.

Důkaz: Jestliže jsou čísla a, b nesoudělná (tedy NSD(a, b) = 1), pak existují celá čísla s, t tak, že $as + bt = 1$. Dále platí $c = sac + tbc$.
Z platnosti $a \mid ab$ a $a \mid bc$ vyplývá $a \mid c$. [6 s. 31] □

Věta 2.5 (Lamé) Počet kroků v Euklidově algoritmu je menší nebo roven pětinásobku počtu číslic menšího z čísel, jejichž NSD hledáme.

Příklad 2.6 Mějme NSD(13578, 4254), počet cifer menšího čísla 4254 se rovná 4. Dále spočítáme $5 \cdot 4 = 20$. Z toho vyplývá, že počet dělení bude menší než 20.

Příklad 2.7 Nalezněte největšího společného dělitele dvou čísel a a b.

$$a = 13578,\ b = 4254,\ \mathrm{NSD}(a,b) = ?$$

Řešení: Provedeme Euklidův algoritmus:

$$13578 = 3 \cdot 4254 + 816$$
$$4254 = 5 \cdot 816 + 174$$
$$816 = 4 \cdot 174 + 120$$
$$174 = 1 \cdot 120 + 54$$
$$120 = 2 \cdot 54 + 12$$
$$54 = 4 \cdot 12 + 6$$
$$12 = 2 \cdot 6 + 0$$

Tabulka Euklidova algoritmu vypadá následovně:

j	–1	0	1	2	3	4	5	6	7
$r_{j-2} - q_j \cdot r_{j-1} =: r_j$	13578	4254	816	174	120	54	12	6	0
q_j			3	5	4	1	2	4	2

NSD(13578, 4254) = 6

Závěr: Našli jsme největšího společného dělitele čísel 13578 a 4254, a tím je číslo 6.

2.2 Historická poznámka

Donald Knuth na začátku knihy [5] popisuje, jak vůbec vzniklo slovo *algoritmus*. Starší podobou slova algoritmus je *algorism*, jehož původ pochází ze jména slavného perského matematika **Muhammada ibn Músá al-Chwárizmího** (přibližně rok 825). Tento matematik sepsal text *Al-Džabr, wa al-Muqabala* (Pravidla pro odvození a srovnání), z názvu mimochodem pochází slovo *algebra*. Název jeho druhé knihy začíná slovy: „*Tak praví al-Chwárizmí*…" V latinském překladu bylo al-Chwárizmího jméno upraveno a text začíná slovy: „*Algoritmi dictit*…" [16 s. 90] Mimochodem tento muž vytvořil praktické postupy pro počítání čísel v desítkové soustavě a podrobné postupy pro řešení rovnic, které se učí ve školách dodnes. Tvar slova *algorism* prošel postupně množstvím etymologických zkomolení až k dnešnímu slovu algoritmus. Do roku 1950 bylo toto slovo nejčastěji spojováno s Euklidovým algoritmem.

Jak už je z názvu patrné, Euklidův algoritmus byl pojmenován podle řeckého matematika **Euklida** (asi 325 př. n. l. – asi 260 př. n. l.)[1]. Postup algoritmu uvedl ve svém díle *Základy*[2] (zhruba 300 př. n. l.). Někteří však tvrdí, že algoritmus sám nevynalezl, ale pouze shromáždil výsledky starších matematiků. Algoritmus pravděpodobně vymyslel **Eudoxos z Knidu** (okolo 375 př. n. l.), jeho vznik však může být datován ještě dříve. Euklidův algoritmus je považován za nejstarší známý algoritmus. Euklides ve svých *Základech* shrnul většinu tehdejších matematických znalostí a tato kniha pak ovlivňovala vývoj matematiky prakticky po dvě tisíciletí. Kromě *Bible* neexistuje žádná kniha, která by vyšla v tolika vydáních a překladech. Stejně jako spousta antických děl i tato kniha byla dochována díky překladům arabských vědců. *Základy* tvoří 13 knih, v prvních šesti knihách se zabývá rovinnou geometrií (trojúhelníky, čtverce, obdélníky,

[1] přesné datum narození a smrti Euklida není známo, někteří historikové datují jeho život mezi Platonovu smrt 374 př.n.l. až narození Archimeda roku 287 př.n.l.
[2] řecky *Stoicheia*, latinsky *Elementa* nebo *Principia*

rovnoběžníky a kružnice), v knihách VII–IX se věnuje teorii čísel, v knize X pojednává o iracionálních číslech a poslední tři knihy věnuje geometrii v prostoru. O životě Euklida se ví velmi málo. Pravděpodobně pocházel z Athén a po příchodu do Alexandrie se stal vedoucím matematické části knihovny, kde pracoval a snad také učil. Dalšími jeho spisy, které se zachovaly díky alexandrijské knihovně, jsou například *Data* o výpočetních postupech, *Optika*, kde položil základy učení o perspektivě, nebo *Základy hudby*, kde shrnul a zpracoval výsledky pythagorejců[3]. Převážně čerpané z [16 s. 59].

[3] členové náboženského spolku, který založil Pythagoras, předmětem bylo studium matematiky a filozofie

3 Rozšířený Euklidův algoritmus a Bézoutova rovnost

Rozšířený Euklidův algoritmus znamená, že k hledání NSD čísel *a, b* přidáme nalezení vyjádření největšího společného dělitele jako celočíselné lineární kombinace vstupních čísel *a* a *b*:

$$\mathrm{NSD}(a, b) = as + bt,$$

čemuž se říká *Bézoutova rovnost*, kde *s* a *t* nazýváme *Bézoutovy koeficienty* nebo *Bézoutova čísla*. Tato čísla nejsou určena jednoznačně.

Bézoutova rovnost je *lineární diofantická rovnice*, což znamená, že se zabýváme pouze celočíselnými řešeními rovnice a neznámé jsou pouze v první mocnině.
Jestliže platí $as + bt = 1$, pak jsou čísla *a*, *b* nesoudělná.

Věta 3.1 (Bézout) Nechť $a, b \in \mathbb{Z}$, potom existují čísla $s, t \in \mathbb{Z}$, že

$$\mathrm{NSD}(a, b) = as + bt.$$

Důkaz: Mějme $d = \mathrm{NSD}(a, b)$. Pokud je $a, b \in \mathbb{N}$, tak rozšířený Euklidův algoritmus dává výsledek. V tomto případě můžeme najít $s, t \in \mathbb{Z}$ tak, že $as + bt = d$. Všimněme si, že

$$(-s)(-a) + tb = sa + (-t)(-b) = (-s)(-a) + (-t)(-b) = d\ .$$

Z toho plyne, že je jednoduché získat výsledek pro $a, b \in \mathbb{Z}$. [12 s. 13] □

3.1 Popis rozšířeného Euklidova algoritmu

V každém kroku algoritmu definujeme $s_j, t_j \in \mathbb{Z}$, že

$$r_j = s_j a + t_j b\ .$$

Nejprve položíme $s_{-1} = 1, t_{-1} = 0$ a $s_0 = 0, t_0 = 1$.

V prvním kroku Euklidova algoritmu $r_1 = r_{-1} - q_1 r_0$ dostáváme

$$s_1 = s_{-1} - q_1 s_0 \text{ a } t_1 = t_{-1} - q_1 t_0\ .$$

V druhém kroku algoritmu $r_2 = r_0 - q_2 r_1$ dostaneme

$$s_2 = s_0 - q_2 s_1 \text{ a } t_2 = t_0 - q_2 t_1 .$$

Tedy pro *j*-tý krok $r_j = r_{j-2} - q_j r_{j-1}$ získáme rovnice

$$s_j = s_{j-2} - q_j s_{j-1} \text{ a } t_j = t_{j-2} - q_j t_{j-1} .$$

Předpoklad, že $s_{j-1}a + t_{j-1}b = r_{j-1}$ a $s_{j-2}a + t_{j-2}b = r_{j-2}$, zajišťuje, že

$$\begin{aligned} s_j a + t_j b &= (s_{j-2} - q_j s_{j-1})a + (t_{j-2} - q_j t_{j-1})b \\ &= s_{j-2}a + t_{j-2}b - q_j (s_{j-1}a + t_{j-1}b) \\ &= r_{j-2} - q_j r_{j-1} \\ &= r_j . \end{aligned}$$

Převzato z [12 s. 12].

Opět můžeme použít tabulku pro výpočet Euklidova algoritmu, kterou rozšíříme o počítání Bézoutových koeficientů:

j	–1	0	1	2	…	n	$n+1$
$r_{j-2} - q_j \cdot r_{j-1} =: r_j$	a	b	r_1	r_2	…	r_n	r_{n+1}
q_j			q_1	q_2	…	q_n	q_{n+1}
$s_{j-2} - q_j \cdot s_{j-1} =: s_j$	1	0	s_1	s_2	…	s_n	s_{n+1}
$t_{j-2} - q_j \cdot t_{j-1} =: t_j$	0	1	t_1	t_2	…	t_n	t_{n+1}

Příklad 3.2 Nalezněte NSD čísel *a, b* a vyjádření největšího společného dělitele jako lineární kombinaci vstupních čísel *a* a *b*.

$a = 13578$, $b = 4254$, NSD(a, b) = ?, s = ?, t = ?

Řešení: Pro výpočet použijeme tabulku:

j	–1	0	1	2	3	4	5	6	7
$r_{j-2} - q_j \cdot r_{j-1} =: r_j$	13578	4254	816	174	120	54	12	6	0
q_j			3	5	4	1	2	4	2
$s_{j-2} - q_j \cdot s_{j-1} =: s_j$	1	0	1	–5	21	–26	73	–318	709
$t_{j-2} - q_j \cdot t_{j-1} =: t_j$	0	1	–3	16	–67	83	–233	1015	–2263

$$\text{NSD}(13578, 4254) = 6$$

$$6 = 13578 \cdot (-318) + 4254 \cdot 1015$$

Závěr: Našli jsme číslo 6 jako největšího společného dělitele čísel 13578 a 4254, dále jsme nalezli koeficienty $s = -318$ a $t = 1015$, a tudíž můžeme NSD vyjádřit jako lineární kombinaci.

3.2 Určení koeficientů *s* a *t*

Pokud chceme stanovit Bézoutovy koeficienty s a t, musíme se vrátit zpět k popisu Euklidova algoritmu. Vezměme upravenou předposlední rovnici algoritmu

$$r_n = r_{n-2} - q_n \cdot r_{n-1}.$$

Tuto rovnici dále upravíme substitucí za r_{n-1}:

$$r_n = r_{n-2} - q_n \cdot (r_{n-3} - q_{n-1} \cdot r_{n-2}) = (1 + q_n \cdot q_{n-1}) \cdot r_{n-2} + (-q_n) \cdot r_{n-3}.$$

Toto reprezentuje r_n jako lineární kombinaci r_{n-2} a r_{n-3}. Zpětným postupem skrz systém rovnic Euklidova algoritmu úspěšně eliminujeme zbytky $r_{n-1}, r_{n-2}, \ldots, r_1, r_0$, až dojdeme k vyjádření, kde r_n = NSD(a, b) jako lineární kombinace a a b. Převzato z [2 s. 27–28].

Příklad 3.3 Mějme NSD(13578, 4254) = 6, nalezněte číslo 6 jako lineární kombinaci čísel 13578 a 4254.

Řešení: Začneme dosazením do rovnice

$$r_n = r_{n-2} - q_n \cdot (r_{n-3} - q_{n-1} \cdot r_{n-2}) = (1 + q_n \cdot q_{n-1}) \cdot r_{n-2} + (-q_n) \cdot r_{n-3}$$

a postupně eliminujeme zbytky 12, 54, 120, 174 a 816.

$$6 = 54 - 4 \cdot 12 = 54 - 4 \cdot (120 - 2 \cdot 54) = (1 + 4 \cdot 2) \cdot 54 + (-4) \cdot 120 = 9 \cdot 54 - 4 \cdot 120$$
$$6 = 9 \cdot (174 - 120) - 4 \cdot 120 = 9 \cdot 174 - 13 \cdot 120$$
$$6 = 9 \cdot 174 - 13 \cdot (816 - 4 \cdot 174) = 61 \cdot 174 - 13 \cdot 816$$
$$6 = 61 \cdot (4254 - 5 \cdot 816) - 13 \cdot 816 = 61 \cdot 4254 - 318 \cdot 816$$
$$6 = 61 \cdot 4254 - 318 \cdot (13578 - 3 \cdot 4254) = 1015 \cdot 4254 - 318 \cdot 13578$$

Závěr: Dostáváme

$$\text{NSD}(13578, 4254) = 6 = 13578 \cdot s + 4254 \cdot t = 13578 \cdot (-318) + 4254 \cdot 1015 .$$

Tím jsme zároveň ověřili náš tabulkový výsledek z příkladu 3.2.

3.3 Rozšířený Euklidův algoritmus pro více čísel

Euklidův algoritmus lze použít nejen pro dvojici čísel, ale můžeme ho rozšířit i na více čísel.

Příklad 3.4 Nalezněte NSD čísel *a, b, c* a vyjádření největšího společného dělitele jako lineární kombinaci vstupních čísel *a, b* a *c*.

$$a = 13578,\ b = 4254,\ c = 136,\ \text{NSD}(13578, 4254, 136) = ?$$

Řešení: V předchozím příkladu jsme již získali největšího společného dělitele 6 čísel 13578 a 4254 a jejich lineární kombinaci. Dále potřebujeme nalézt největšího společného dělitele čísel 136 a 6, tedy třetího čísla *c* a NSD(*a*, *b*). Výsledek získáme opět použitím tabulky.

j	-1	0	1	2	3
$r_{j-2} - q_j \cdot r_{j-1} =: r_j$	136	6	4	2	0
q_j			22	1	2
$s_{j-2} - q_j \cdot s_{j-1} =: s_j$	1	0	1	-1	2
$t_{j-2} - q_j \cdot t_{j-1} =: t_j$	0	1	-22	23	-68

$$\text{NSD}(136, 6) = 2$$

$$2 = 136 \cdot (-1) + 6 \cdot 23$$

Závěr: Získali jsme tedy jak NSD tak i Bézoutovu rovnost. Takže

$$\text{NSD}(13578, 4254, 136) = 2$$

a jeho lineární kombinaci můžeme zapsat takto:

$$\text{NSD}(a, b, c) = as + bt + cu$$

$$2 = 136 \cdot (-1) + \left[13578 \cdot (-318) + 4254 \cdot 1015\right] \cdot 23$$

$$2 = 136 \cdot (-1) + 13578 \cdot (-7314) + 4254 \cdot 23345 .$$

3.4 Historická poznámka

Euklidův algoritmus byl nezávisle objeven také ve starověké Indii a Číně především k řešení diofantických rovnic používaných při výpočtech v astronomii a k tvorbě přesného kalendáře. Jak indičtí tak čínští matematici mají velkou zásluhu na vymezení otázky celočíselného řešení neurčitých[4] rovnic. Nesmíme opomenout ani **Diofanta z Alexandrie** (asi 200 – asi 284 n. l.), podle kterého se právě část teorie čísel nazývá diofantické rovnice. On sám ale nepožadoval celočíselnost řešení, vystačil si s racionálním řešením.

Metoda nalezení celočíselného řešení rovnice $as - bt = 1$ známé jako Bézoutova rovnost byla popsána roku 1624 francouzským matematikem **Claudem Gespard Bachetem** v jeho knize *Problèmes plaisants et délectables*, kde základ problému popisuje v tvrzení XVIII: „Jsou dána dvě prvočísla, nejmenší násobek každého z nich se nalezne tak, že jedno prvočíslo předčí druhé jednotkou.“ [3 s. 122]
Etiènne Bézout následoval Bacheta a roku 1766 napsal *Cours d'Algèbre*, kde metodu ilustroval na následujícím příkladu.

Příklad 3.5 Kolika možnými způsoby lze zaplatit částku 542 liver[5], platí-li se mincemi v hodnotě 17 liver a na to je vraceno 11livrovými mincemi?

Řešení: Tento problém lze zapsat rovnicí $17x - 11y = 542$ a vyjádřením y z rovnice dostaneme $y = \frac{17x - 542}{11}$. Zvolením libovolného x dostaneme vždy hodnotu y, která splňuje rovnici, v otázce je však požadováno, aby x a y byla celá čísla. Rovnice $y = \frac{17x - 542}{11}$ může být upravena provedením dělení tak, že

$$y = x - 49 + \frac{6x - 3}{11}.$$

[4] označení *neurčitá* znamená, že rovnice má více neznámých
[5] Livra byla francouzská měna používaná do roku 1795

Provedeme několik substitucí a úprav dělením:

$$u = \frac{6x-3}{11} \quad \rightarrow \quad x = \frac{11u+3}{6} = u + \frac{5u+3}{6}$$
$$t = \frac{5u+3}{6} \quad \rightarrow \quad u = \frac{6t-3}{5} = t + \frac{t-3}{5}$$
$$s = \frac{t-3}{5} \quad \rightarrow \quad t = 5s+3, \quad \text{kde } u, t, s \text{ musí být celá čísla.}$$

Operace končí u $t = 5s+3$, protože je jasné, že zvolením jakéhokoli celého čísla za *s* bude *t* vždy celé číslo.

Teď zpětně dosadíme do $x = \frac{11u+3}{6} = \frac{66t-33+15}{30} = \frac{330s+198-18}{30} = 11s+6$

a následně dosadíme získanou hodnotu $x = 11s+6$ do rovnice

$$y = \frac{17x-542}{11} = \frac{187s+102-542}{11} = 17s-40.$$

Závěr: Získali jsme odpovídající hodnoty pro *x* a *y*:

$$x = 11s+6 \text{ a } y = 17s-40.$$

U první hodnoty *x* může být za *s* zvoleno libovolné číslo, ale u druhé hodnoty *y* nesmí být *s* menší než 3, protože *y* by nebylo kladné.

Rovnice $17x-11y = 542$ je splněna nekonečným počtem možností pro s = 3, 4, 5,…

$$s = 3: \quad x = 39,\ y = 11$$
$$s = 4: \quad x = 50,\ y = 28$$
$$s = 5: \quad x = 61,\ y = 45, \quad \text{atd.}$$

Příklad převzat z [3 s. 123–124].

4 Výpočet inverzního prvku

Pomocí rozšířeného Euklidova algoritmu lze vypočítat inverzní prvek k b modulo m. Inverzní prvek b^{-1} k prvku b je takový prvek, který po vynásobení s b dá neutrální prvek modulo m.

$$b \cdot b^{-1} = b^{-1} \cdot b \equiv_m 1$$

Definice 4.1 Pokud a a b dávají stejný zbytek po dělení m, tj. pokud $m \mid a - b$, budeme psát $a \equiv_m b$ (čteme a je kongruentní s b modulo m).

Další možné značení kongruence je $a \equiv b \pmod{m}$.

Poznámka 4.2 Relace „býti kongruentní modulo m“ je ekvivalence, je tedy reflexivní[6], symetrická[7] a tranzitivní[8].

Inverzní prvek můžeme určit z lineární diofantické rovnice nazývané Bézoutova rovnost. Podmínkou zde je, že největší společný dělitel čísel a, b je roven jedné.

$$a \cdot s + b \cdot t = 1$$

Pokud by byl NSD(a, b) > 1, a nemá inverzní prvek modulo b.

Věta 4.3 Celé číslo a má inverzní prvek modulo b, právě když je a a b nesoudělné.

Důkaz: Předpokládejme, že a má takový inverzní prvek, že platí $ac \equiv 1 \pmod{b}$. Pak $b \mid (ac - 1)$ značí $bx = ac - 1$, což můžeme přepsat jako $1 = ac - bx$. Z toho plyne, že a a b jsou nesoudělná. Potom je $1 = \text{NSD}(a, b) = as + bt$, tedy $1 - as = bt$, a z toho dostáváme, že $b \mid (1 - as)$. To je $1 \equiv as \pmod{b}$, takže s je inverzní prvek čísla a modulo b. [14 s. 57] □

[6] $\forall\, a \in A$ platí $(a, a) \in R$, kde R je relace na množině A

[7] $\forall\, a, b \in A$ platí $(a, b) \in R \Rightarrow (b, a) \in R$, kde R je relace na množině A

[8] $\forall\, a, b, c \in A$ platí $(a, b) \in R \wedge (b, c) \in R \Rightarrow (a, c) \in R$, kde R je relace na množině A

Příklad 4.4 Vypočtěte inverzní prvek ke 203 modulo 250.

Řešení: Nejdříve vypočítáme rozšířený Euklidův algoritmus pro čísla 250 a 203.

j	–1	0	1	2	3	4
$r_{j-2} - q_j \cdot r_{j-1} =: r_j$	250	203	47	15	2	1
q_j			1	4	3	7
$s_{j-2} - q_j \cdot s_{j-1} =: s_j$	1	0	1	–4	13	–95
$t_{j-2} - q_j \cdot t_{j-1} =: t_j$	0	1	–1	5	–16	117

Získali jsme největšího společného dělitele a jejich lineární kombinaci, z té získáme inverzní prvek čísla 203.

$$\mathrm{NSD}(250, 203) = 1$$

$$1 = 250 \cdot (-95) + 203 \cdot 117$$
$$\xrightarrow{\text{mod } 250} \quad 0 + 203 \cdot 117 \equiv_{250} 1 \Rightarrow 203^{-1} \equiv_{250} 117$$

Závěr: Inverzní prvek k číslu 203 modulo 250 je číslo 117.

4.1 Zbytkové třídy modulo *m*

Relace „modulo *m*“ definuje rozklad $\mathbb{Z}$ na množinu $\mathbb{Z}_m = \{[0], [1],\ldots,[m-1]\}$, kde $\mathbb{Z}_m$ je množina zbytkových tříd modulo *m*, každá třída je množina celých čísel, které při dělení přirozeným číslem *m* dávají stejný zbytek. Rozklad se značí $\mathbb{Z} / \mathbb{Z}_m$ a má *m* tříd. Jako reprezentanta třídy ekvivalence lze vzít libovolný prvek z dané třídy, nejčastěji bereme nejmenší nezáporný prvek.

Tvrzení 4.5 Jestliže NSD(*a*, *m*) = 1, pak lze nalézt $b \in \mathbb{Z}_m$ takové, že

$$a \cdot b \equiv 1 \pmod{m},$$

tzn. že prvky *a*, *b* jsou k sobě inverzní.

Speciálně platí pro množinu $\mathbb{Z}_p$, kde *p* je prvočíslo, že všechny prvky množiny $\mathbb{Z}_p \setminus \{0\}$ jsou nesoudělné s *p*.

Definice 4.6 Jestliže n, m jsou celá čísla a $m > 0$, pak definujeme

$$n \equiv n - \lfloor n/m \rfloor m \pmod{m}.$$

Po úpravě dostaneme $n \equiv \lfloor n/m \rfloor m + n \pmod{m}$. Pokud budeme n dělit m, pak dostaneme podíl $q = \lfloor n/m \rfloor$ a zbytek $r \equiv n \pmod{m}$. [14 s. 39]

(Pozn.: $\lfloor n/m \rfloor$ je dolní celá část[9] čísla n/m)

Příklad 4.7 Je-li zadáno $n = 57$ a $m = 9$, pak podle definice 4.6 spočítáme

$$57 \equiv 57 - \lfloor 57/9 \rfloor 9 \pmod{9}$$
$$57 - 6 \cdot 9 = 57 - 54 = 3.$$

4.2 Euklidův algoritmus a největší společný dělitel

Euklidův algoritmus pro výpočet největšího společného dělitele čísel a, b v modulární aritmetice: mějme posloupnost zbytků

$$r_0 \equiv a \pmod{b}$$
$$r_1 \equiv b \pmod{r_1}$$
$$\vdots$$
$$r_{n+1} \equiv r_{n-1} \pmod{r_n},$$

poslední zbytek nám dává NSD(a, b).

Věta 4.8 Jestliže a, b jsou celá čísla a $b > 0$, pak platí

$$\text{NSD}(a, b) = \text{NSD}(a \bmod b, b).$$

Protože jednou z vlastností největšího společného dělitele je komutativita NSD(a, b) = NSD(b, a), můžeme psát

$$\text{NSD}(a, b) = \text{NSD}(b, a \bmod b).$$

Převzato z [14 s. 44].

Příklad 4.9 Spočítejte NSD(24, 54).

NSD(54, 24) = NSD(24, 54 mod 24) = NSD(24, 6) = NSD(6, 24 mod 6) =
= NSD(6, 0) = 6

[9] jestliže $x \in \mathbb{R}$, tak $\lfloor x \rfloor$ je největší celé číslo menší nebo rovné x

4.3 RSA algoritmus

Euklidův algoritmus má uplatnění i v asymetrickém šifrování, které slouží k zabezpečení informací. Metoda RSA (zkratka složená z prvních písmen autorů Rivers, Shamir, Adleman) je první asymetrickou šifrou, byla publikována roku 1978 a používá se pro šifrování i pro podepisování dokumentů. Asymetrická šifra má k šifrování dva klíče, veřejný k zašifrování a soukromý k odšifrování. Zašifrovanou zprávu nelze bez klíče rozluštit ani v případě, že známe způsob kódování. Běžně se využívá pro datový přenos na internetu. RSA algoritmus je založen na skutečnosti, že vynásobení dvou prvočísel velkého řádu je na počítači běžným úkonem, ale provést zpětné rozložení je prakticky nemožné. Euklidův algoritmus se používá v kroku, kdy je potřeba určit inverzní prvek.

4.3.1 Vlastní algoritmus RSA

Zde si ve zkratce uvedeme zjednodušený vlastní algoritmus metody RSA.

1) Generování páru klíčů

- Zvolíme si dvě prvočísla p a q a vypočítáme jejich součin $n = pq$.
- Dále určíme hodnotu Eulerovy funkce[10] $\varphi(n) = \varphi(pq) = (p-1)(q-1)$.
- Nalezneme celé číslo d takové, že $\mathrm{NSD}(\varphi(n), d) = 1$.
- Vypočítáme číslo e tak, aby platilo $e \cdot d \equiv_{\varphi(n)} 1$, tedy $e \equiv_{\varphi(n)} d^{-1}$.
- Tím nám vznikla dvojice (e, n) pro veřejný klíč a soukromý klíč je dán dvojicí (d, n).

2) Zašifrování, odšifrování

- Mějme x jako text zprávy pro zašifrování a c nechť je zašifrovaný text.
- Chceme-li zprávu zašifrovat, použijeme vzorec $c \equiv_n x^e$, naopak potřebujeme-li zprávu odšifrovat, použijeme vzorec $x \equiv_n c^d$.

[10] Eulerova funkce $\varphi(n)$ udává počet přirozených čísel k menších než n, pro něž platí $\mathrm{NSD}(k, n) = 1$ tedy $k \perp n$

5 Řetězové zlomky

Euklidův algoritmus také slouží k nalezení řetězového zlomku ke kladnému racionálnímu číslu *m*/*n*.

Řetězovým zlomkem nazýváme výraz

$$a_1 + \cfrac{b_1}{a_2 + \cfrac{b_2}{a_3 + \cfrac{b_3}{a_4 + \ldots}}},$$

kde a_j a b_j pro $j = 1, 2, \ldots$ jsou reálná nebo komplexní čísla. Každé racionální číslo lze obecně vyjádřit jako řetězový zlomek. Zlomek, který má konečný počet prvků, se nazývá konečný řetězový zlomek (všechna racionální čísla). Výraz, kde se prvky b_j rovnají jedné, pojmenujeme pravidelný řetězový zlomek. Zde můžeme použít jednodušší zápis řetězového zlomku $\langle a_1, a_2, a_3, a_4, \ldots, a_n \rangle$, kde čísla $a_1, \ldots, a_n$ nazveme prvky řetězového zlomku nebo také neúplné podíly. Zlomek, který má nekonečný počet prvků, se nazývá nekonečný řetězový zlomek (iracionální čísla). Dále můžeme řetězové zlomky rozdělit na periodické a neperiodické.

5.1 Euklidův algoritmus pro racionální číslo m/n

Zde jsou prvky řetězového zlomku a_j označeny jako q_j a prvky b_j jsou rovny jedné.

$$m = q_1 n + r_1 \quad \rightarrow \quad \frac{m}{n} = q_1 + \frac{r_1}{n} \quad \rightarrow \quad \frac{m}{n} = q_1 + \cfrac{1}{\cfrac{n}{r_1}}$$

$$n = q_2 r_1 + r_2 \quad \rightarrow \quad \frac{n}{r_1} = q_2 + \frac{r_2}{r_1} \quad \rightarrow \quad \frac{n}{r_1} = q_2 + \cfrac{1}{\cfrac{r_1}{r_2}}$$

$$\vdots$$

$$r_{n-2} = q_n r_{n-1} + r_n \quad \rightarrow \quad \frac{r_{n-2}}{r_{n-1}} = q_n + \frac{r_n}{r_{n-1}} \quad \rightarrow \quad \frac{r_{n-2}}{r_{n-1}} = q_n + \cfrac{1}{\cfrac{r_{n-1}}{r_n}}$$

$$r_{n-1} = q_{n+1} r_n + 0 \quad \rightarrow \quad \frac{r_{n-1}}{r_n} = q_{n+1} + 0$$

Všechny rovnosti Euklidova algoritmu jsme upravili dělením, budeme-li postupně vkládat druhou rovnici $\frac{n}{r_1}$ do první rovnice $\frac{m}{n}$, třetí rovnici $\frac{r_1}{r_2}$ do druhé, čtvrtou rovnici do třetí a tak dále až vložíme poslední rovnici, dostaneme hledaný řetězový zlomek, který bude tvaru

$$q_1 + \cfrac{1}{q_2 + \cfrac{1}{q_3 + \cfrac{1}{q_4 + \ldots + \cfrac{1}{q_{n+1}}}}}.$$

Vyjádření racionálního čísla řetězovým zlomkem je jednoznačné právě tehdy, platí-li pro poslední prvek $q_{n+1} > 1$ (tedy nesmí být roven jedné), toto plyne z rovností Euklidova algoritmu.

K řetězovému zlomku $\langle q_1, q_2, q_3, q_4, \ldots, q_{n+1} \rangle$ můžeme vypočítat konvergenty, též nazývané sblížené zlomky. Konvergenta aproximuje řetězový zlomek, čím je dál, tím je přesnější. Pro čitatele m_j a jmenovatele n_j sblíženého zlomku platí rekurentní vzorce

$$\begin{aligned} m_1 &= q_1, \quad n_1 = 1 \\ m_2 &= q_1 \cdot q_2 + 1, \quad n_2 = q_2 \\ m_j &= q_j \cdot m_{j-1} + m_{j-2}, \quad j \geq 3 \\ n_j &= q_j \cdot n_{j-1} + n_{j-2}, \quad j \geq 3 \end{aligned}.$$

Vztahy pro m_1, n_1, m_2, n_2 získáme z obecných vztahů pro m_j, n_j, jestliže položíme $m_0 = 1, m_{-1} = 0, n_0 = 0, n_{-1} = 1$.

Převzato z [17 s. 24]

Příklad 5.1 Vyjádřete racionální číslo 392/905 jako řetězový zlomek a vypočtěte konvergenty.

Řešení: Opět zde využijeme tabulku pro rozšířený Euklidův algoritmus, ale s několika malými změnami (označeny červeně).

j	–1	0	1	2	3	4	5	6	7
$r_{j-2} - q_j \cdot r_{j-1} =: r_j$	392	905	392	121	29	5	4	1	0
q_j			0	2	3	4	5	1	4
$m_{j-2} + q_j \cdot m_{j-1} =: m_j$	0	1	0	1	3	13	68	81	392
$n_{j-2} + q_j \cdot n_{j-1} =: n_j$	1	0	1	2	7	30	157	187	905
$c_j = m_j / n_j$			0	$\frac{1}{2}$	$\frac{3}{7}$	$\frac{13}{30}$	$\frac{68}{157}$	$\frac{81}{187}$	$\frac{392}{905}$

Z rovností Euklidova algoritmu dostaneme řetězový zlomek čísla 392/905 takto:

$$\frac{392}{905} = 0 + \frac{1}{\frac{905}{392}} = 0 + \frac{1}{2 + \frac{1}{\frac{392}{121}}} = 0 + \frac{1}{2 + \frac{1}{3 + \frac{1}{\frac{121}{29}}}} = 0 + \frac{1}{2 + \frac{1}{3 + \frac{1}{4 + \frac{1}{\frac{29}{5}}}}} =$$

$$= 0 + \frac{1}{2 + \frac{1}{3 + \frac{1}{4 + \frac{1}{5 + \frac{1}{\frac{5}{4}}}}}} = 0 + \frac{1}{2 + \frac{1}{3 + \frac{1}{4 + \frac{1}{5 + \frac{1}{1 + \frac{1}{4}}}}}}$$

Zjednodušený zápis: $392/905 = \langle q_1, q_2, q_3, q_4, q_5, q_6, q_7 \rangle = \langle 0, 2, 3, 4, 5, 1, 4 \rangle$

Konvergenty c_j vyčteme z posledního řádku tabulky.

$$\left(c_j\right)_{j=1}^{7} = \left(0, \frac{1}{2}, \frac{3}{7}, \frac{13}{30}, \frac{68}{157}, \frac{81}{187}, \frac{392}{905}\right)$$
$$\approx (0; 0{,}5; 0{,}428571; 0{,}433333; 0{,}433121; 0{,}433155; 0{,}433149)$$

5.2 Řešení kongruence řetězovými zlomky

Pomocí řetězových zlomků můžeme řešit kongruence typu

$$ax \equiv b \pmod{d}$$

za předpokladu, že NSD(a, d) = 1, kdy použijeme řetězový zlomek racionálního čísla d/a. Po úpravách, které naleznete například v [17 s. 129], dostaneme řešení

$$x \equiv (-1)^n m_n b \pmod{d}.$$

Jestliže takto vypočítané x není prvkem soustavy $\{0, 1, \ldots, d-1\}$, dostaneme x_0 přičtením dt, kde t je vhodné celé číslo.

Příklad 5.2 Řešte kongruenci

$$37x \equiv 7 \pmod{121}.$$

Řešení: Čísla 37, 121 jsou přirozená čísla a nesoudělná. Vypočítáme nejprve prvky řetězového zlomku čísla 121/37:

j	-1	0	1	2	3	4	5
$r_{j-2} - q_j \cdot r_{j-1} =: r_j$	121	37	10	7	3	1	0
q_j			3	3	1	2	3
$m_{j-2} + q_j \cdot m_{j-1} =: m_j$	0	1	3	10	13	36	121
$n_{j-2} + q_j \cdot n_{j-1} =: n_j$	1	0	1	3	4	11	37

$$\begin{aligned} m_n &= m_4 = 36 \\ x &\equiv (-1)^n m_n b \pmod{d} \equiv (-1)^4 36 \cdot 7 \pmod{121} \\ x &\equiv 252 \pmod{121} \\ x_0 &= 252 - 2 \cdot 121 = 10 \end{aligned}$$

Závěr: Řešením zadané kongruence je číslo 10.

Příklad inspirován příkladem [17 s. 130–131].

5.3 Historická poznámka

O zjednodušení zlomků velkých čísel se jako první pokoušeli **Aristarchos ze Samu** nebo **Archimédes**. Francouzský historik matematiky Jean Itard zrekonstruoval Aristarchovo použití algoritmu pro zjednodušení zlomku A/B, kde A = 71755875, B = 61735500 takto:

$$A - B = C = 10020375$$
$$B - 6C = D = 1613250$$
$$C - 6D = 340875$$

Zanedbáním posledního zbytku dostaneme

$$C = 6D,\ B = 6C + D = 37D,\ A = B + C = 43D \rightarrow A/B \approx 43/37 .$$

Více v [3 s. 117].

Zárodek idey řetězových zlomků obsahuje Kniha X Euklidových *Základů*, tvrzení 2 o nesouměřitelných veličinách. V teoretickém rozvoji této myšlenky pokračovali perští matematici **al-Máhání** (9. století) a **al-Khayyám** (12. století), kteří ukázali rovnost dvou zlomků uvážením posloupnosti postupných podílů získaných aplikací Euklidova algoritmu na každý zlomek zvlášť a dokázali, že jejich rozvoje v řetězový zlomek jsou identické. [3 s. 126–127]

Definice rovnosti dvou zlomků podle Al-Khayyámova textu

Mějme čtyři veličiny *a*, *b*, *c*, *d* tak, že pro ně platí jeden ze tří předpokladů:

1) $a = b$ a $c = d$

2) $a = \frac{b}{n}$ a $c = \frac{d}{n}$

3) $a = \frac{k}{n} b$ a $c = \frac{k}{n} d$,

kde *n*, *k* jsou celá čísla. Pak pro všechny tyto případy platí, že zlomky $\frac{a}{b}$ a $\frac{c}{d}$ si jsou rovny.

Máme-li jakékoli veličiny, pro které platí

4) $b - n_1 a = p_1$, kde $p_1 < a$ a $d - n_1 c = q_1$, kde $q_1 < c$,

$a - n_2 p_1 = p_2$, kde $p_2 < p_1$ a $c - n_2 q_1 = q_2$, kde $q_2 < q_1$,

$$p_1 - n_3 p_2 = p_3, \text{ kde } p_3 < p_2 \text{ a } q_1 - n_3 q_2 = q_3, \text{ kde } q_3 < q_2, \text{ atd.}$$

Jestliže je v každém *k*-tém kroku prvek n_k stejný v obou nerovnostech, pak jsou zlomky $\frac{a}{b}$ a $\frac{c}{d}$ rovny. Převzato z [3 s. 120].

Řetězové zlomky se používaly také ve starověké Číně (3.–4. st.) a Indii (5. st.) k řešení neurčitých rovnic. Prvním podnětem k řešení těchto rovnic byly astronomické výpočty kalendáře, kde bylo potřeba určit periodu opakování stejných relativních postavení nebeských těles s různými dobami oběhu a jiné s tím související problémy. K určení prvků řetězového zlomku používali Euklidův algoritmus. [18 s. 143–145]

Ideou řetězových zlomků se dále zabývali například **Gottfried Wilhelm Leibniz** (17.–18. st.) a **Christiaan Huygens** (17. st.), který řetězové zlomky použil při výpočtech konstrukce svého planetária. Teorie řetězových zlomků, jak ji známe dnes, vznikla v 18. století a jejím zakladatelem je **Leonhard Euler**, kterého doplnil **Joseph Louis Lagrange**.

6 Euklidův algoritmus pro polynomy

Polynom neboli mnohočlen je výraz ve tvaru

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + a_{n-2} x^{n-2} + \ldots + a_2 x^2 + a_1 x^1 + a_0 x^0,$$

kde $a_n, a_{n-1}, \ldots, a_0$ se nazývají *koeficienty polynomu* a $a_n x^n$ se nazývá *vedoucí člen* a $a_0 x^0$ *absolutní člen*. Polynom můžeme zapsat také ve zkráceném tvaru

$$\sum_{j=1}^{n} a_j x^j .$$

Pokud je koeficient a_n různý od nuly, pak má polynom stupeň n[11]. Podobně jako u celých čísel můžeme i u polynomů určit největšího společného dělitele, a to opět skrze Euklidův algoritmus. Základ algoritmu je analogický.
Největší společný dělitel dvou polynomů $f(x)$, $g(x)$ je definován jako součin jejich společných *ireducibilních polynomů*, který nalezneme právě použitím Euklidova algoritmu.

Ireducibilní polynom je analogií prvočísla, každý polynom lze vyjádřit jako součin mocnin ireducibilních polynomů a ireducibilní polynom nelze rozložit na součin polynomů nižšího stupně. Ireducibilní polynom má pouze triviální dělitele. V reálném oboru jsou ireducibilní právě polynomy stupně 1 a ty polynomy stupně 2, které nemají reálný kořen.

Věta 6.1 (O dělení se zbytkem) Nechť $f(x)$ a $g(x)$ jsou polynomy jedné neurčité x nad tělesem T, kde T je komutativní, a $g(x) \neq 0$. Pak v $T[x]$ existují polynomy $q(x)$, $r(x)$ takové, že $f(x) = g(x)q(x) + r(x)$, kde $r(x) = 0$ nebo $\mathrm{st}(r) < \mathrm{st}(g)$. Polynomy $q(x)$, $r(x)$ jsou těmito podmínkami určeny jednoznačně. [9 s. 28]

Definice 6.2 Nechť $f_1(x), f_2(x), \ldots, f_n(x) \in T[x]$. Polynom $d(x) \in T[x]$ nazveme největším společným dělitelem polynomů $f_1(x), f_2(x), \ldots, f_n(x)$, jestliže platí:
1) $d(x) \mid f_j(x)$ pro každé $j = 1, 2, \ldots, n$.
2) Jestliže $h(x) \in T[x]$ a $h(x) \mid f_j(x)$ pro každé $j = 1, 2, \ldots, n$, pak $h(x) \mid d(x)$.
[9 s. 28]

[11] stupeň polynomu je nejvyšší exponent proměnné x s nenulovým koeficientem

6.1 Euklidův algoritmus a Bézoutova rovnost

Nechť polynomy $f(x)$, $g(x) \in T[x]$. Jestliže $f(x) \mid g(x)$, resp. $g(x) \mid h(x)$, je NSD($f(x)$, $g(x)$) = $f(x)$, resp. NSD($f(x)$, $g(x)$) = $g(x)$.

Nechť $f(x)$ nedělí $g(x)$ a naopak. Polynom $f(x)$ vydělíme $g(x)$. Podle věty 6.1 dostaneme částečný podíl $q_1(x)$ a zbytek $r_1(x)$:

(Pozn.: Pro zjednodušení a přehlednost použijeme v rovnicích označení f, g, q_j, r_j)

$$f = gq_1 + r_1, \ \mathrm{st}(r_1) < \mathrm{st}(g).$$

Protože $g(x)$ nedělí $f(x)$, platí $r_1(x) \neq 0$. Opět použijeme větu 6.1:

$$g = r_1 q_2 + r_2, \ \mathrm{st}(r_2) < \mathrm{st}(r_1).$$

Toto postupné dělení provádíme tak, že obecně v j-tém kroku dělíme

$$r_{j-2} = r_{j-1} q_j + r_j, \ \mathrm{st}(r_j) < \mathrm{st}(r_{j-1}).$$

Pro konečný počet kroků dostáváme algoritmus:

$$\begin{aligned} f &= gq_1 + r_1 \\ g &= r_1 q_2 + r_2 \\ &\vdots \\ r_{n-2} &= r_{n-1} q_n + r_n \\ r_{n-1} &= r_n q_{n+1} \end{aligned}$$

kde

$$\mathrm{st}(g) > \mathrm{st}(r_1) > \ldots > \mathrm{st}(\mathrm{st}(r_n)) \geq 0.$$

Potom platí

$$r_n = \mathrm{NSD}(f, g).$$

[9 s. 29]

Věta 6.3 (Bézoutova rovnost) Nechť $f(x)$, $g(x) \in T[x]$. Potom existují polynomy $s(x)$, $t(x) \in T[x]$ tak, že platí

$$\mathrm{NSD}(f(x), g(x)) = f(x)s(x) + g(x)t(x).$$

[9 s. 29]

Příklad 6.4 Nalezněte největšího společného dělitele polynomů $f(x)$, $g(x)$ a zjistěte jejich lineární kombinaci (Bézoutovu rovnost).

$$f(x) = 8x^4 - 8x^3 + 6x - 6, \quad g(x) = 4x^4 - 16x^3 + 12x^2 + 6x - 6$$

Řešení: Euklidův algoritmus bude mít čtyři kroky.

$$f = q_1 g + r_1 \rightarrow 8x^4 - 8x^3 + 6x - 6 = 2 \cdot (4x^4 - 16x^3 + 12x^2 + 6x - 6) + \\ + (24x^3 - 24x^2 - 6x + 6)$$

$$g = q_2 r_1 + r_2 \rightarrow 4x^4 - 16x^3 + 12x^2 + 6x - 6 = (\frac{1}{6}x - \frac{1}{2}) \cdot (24x^3 - 24x^2 - 6x + 6) + \\ + (x^2 + 2x - 3)$$

$$r_1 = q_3 r_2 + r_3 \rightarrow 24x^3 - 24x^2 - 6x + 6 = (24x - 70) \cdot (x^2 + 2x - 3) + (210x - 210)$$

$$r_2 = q_4 r_3 + r_4 \rightarrow x^2 + 2x - 3 = (\frac{1}{210}x + \frac{1}{70}) \cdot (210x - 210) + 0$$

NSD($f(x)$, $g(x)$) = $r_3 = 210x - 210 = 210(x - 1)$

Pro polynomy můžeme také využít tabulku pro rozšířený Euklidův algoritmus (tabulka je tentokrát pro lepší zápis ve sloupcovém tvaru rozdělená na dvě části: základní algoritmus a rozšířená část pro výpočet Bézoutových koeficientů).

j	r_j	q_j
–1	$8x^4 - 8x^3 + 6x - 6$	
0	$4x^4 - 16x^3 + 12x^2 + 6x - 6$	
1	$24x^3 - 24x^2 - 6x + 6$	2
2	$x^2 + 2x - 3$	$\frac{1}{6}x - \frac{1}{2}$
3	$210x - 210$	$24x - 70$
4	0	$\frac{1}{210}x + \frac{1}{70}$

j	s_j	t_j
–1	1	0
0	0	1
1	1	–2
2	$-\frac{1}{6}x + \frac{1}{2}$	$\frac{1}{3}x$
3	$4x^2 - 24x + 37$	$-8x^2 + 24x - 2$
4	$-\frac{2}{105}x^3 + \frac{2}{35}x^2 - \frac{1}{35}$	$\frac{4}{105}x^3 + \frac{1}{35}$

Bézoutova rovnost:

$$210x - 210 = 210(x-1) = (8x^4 - 8x^3 + 6x - 6)(4x^2 - 24x + 37) +$$
$$+ (4x^4 - 16x^3 + 12x^2 + 6x - 6)(-8x^2 + 24x - 2)$$

Rozklad na ireducibilní polynomy:

$$f(x) = 8x^4 - 8x^3 + 6x - 6 = 2(x-1)(4x^3 + 3)$$
$$g(x) = 4x^4 - 16x^3 + 12x^2 + 6x - 6 = 2(x-1)(2x^3 - 6x^2 + 3)$$

NSD($f(x)$, $g(x)$) = $2x - 2 = 2(x - 1)$

Závěr: Je vidět, že Euklidovým algoritmem i rozkladem na ireducibilní polynomy získáme stejného společné dělitele až na násobek. Z algebry ale víme, že tyto polynomy si jsou rovny.

7 Čínská zbytková věta

Vyřešit jednoduchou lineární diofantickou rovnici není těžké, jak ale najít společné řešení několika takových rovnic? Tento problém řešil již čínský matematik **Sun Tsu**, který nalezl metodu určující celá čísla, která mají zbytky 2, 3, 2, když jsou dělena čísly 3, 5, 7. Hledal tedy řešení lineárních rovnic pro přirozená čísla m_1, m_2, m_3:

$$x = 3m_1 + 2 \quad x = 5m_2 + 3 \quad x = 7m_3 + 2 .$$

Sun Tsu spočítal, že řešením je $x = 233 = 3 \cdot 77 + 2 = 5 \cdot 46 + 3 = 7 \cdot 33 + 2$. Nicméně číslo 233 není nejmenším řešením. Odstraníme-li z něj násobky čísel 3, 5, 7, tedy $3 \cdot 5 \cdot 7 = 105$, dostaneme $x = 233 - 2 \cdot 105 = 23$. Číslo 23 je jednoznačně nejmenší kladné celé číslo. [11 s. 40]

Věta 7.1 Předpokládejme, že $n > 1$ je celé číslo, $m_j \in \mathbb{N}$ pro přirozená čísla $j \leq n$ jsou po dvou nesoudělná, a $r_j \in \mathbb{Z}$ pro $j \leq n$ jsou libovolná. Potom existují celá čísla x_j pro $1 \leq j \leq n$ tak, že

$$m_1 x_1 + r_1 = m_2 x_2 + r_2 = \ldots = m_n x_n + r_n .$$

Vidíme, že tato věta zobecňuje problém matematika Sun Tsu. Říká, že pro daná po dvou nesoudělná čísla m_1, m_2,…, m_n pro $n \geq 2$ a libovolná čísla r_1, r_2,…, r_n existuje celé číslo x takové, že dělením x čísly m_1, m_2,…, m_n získáváme zbytky r_1, r_2,…, r_n.
Převzato z [11 s. 40–41].

Příklad 7.2 (Problém s kokosy) Tři námořníci a jedna opice ztroskotali na ostrově. Námořníci nasbírali n kokosů jako zásobu jídla a uložili je na hromadu. Během noci jeden z námořníků vstal a z hromady kokosů, kterou rozdělil na tři hromady, si vzal svůj spravedlivý podíl. Při rozdělování mu zbyl jeden kokos, který dal opici. Svůj podíl si schoval a šel spát. Oba zbylí námořníci udělali stejnou věc jako první námořník. Ráno si námořníci rozdělili zbývající hromádku

a opici dali její čtvrtý kokos. Jaký je minimální počet kokosů, který by mohl být v původní hromadě kokosů?

Řešení: První námořník začal s hromadou $y = 3m_1 + 1$ kokosů.

Druhý námořník pokračoval s hromadou kokosů, kterých bylo

$$y_1 = \frac{2(y-1)}{3} = 3m_2 + 1,$$

a třetí námořník pokračoval s množstvím kokosů

$$y_2 = \frac{2(y_1-1)}{3} = 3m_3 + 1.$$

Ráno rozdělili zbývající hromadu kokosů

$$y_3 = \frac{2(y_2-1)}{3} = 3m_4 + 1.$$

Z výše uvedených rovnic spočítáme y_3 a dostaneme

$$y_3 = \frac{8}{27}y - \frac{38}{27} = 3m_4 + 1.$$

Úpravou rovnice $\frac{8}{27}y - \frac{38}{27} = 3m_4 + 1$ vynásobením obou stran 27 dostaneme

$$8y = 81m_4 + 65.$$

Aby byl výraz $81m_4 + 65$ dělitelný 8 (což $80m_4$ určitě je), musí být $m_4 + 65$ dělitelné 8. Nejmenší kladnou hodnotou m_4 je 7, tudíž po dosazení do rovnice $8y = 81m_4 + 65$ dostáváme y = 79.

Věta 7.3 Předpokládejme, že $m_1, m_2, \ldots, m_n$ jsou (ne nutně nesoudělná) přirozená čísla a $r_1, r_2, \ldots, r_n$ jsou libovolně vybraná celá čísla. Potom má systém rovnic

$$x = m_1x_1 + r_1 = m_2x_2 + r_2 = \ldots = m_nx_n + r_n$$

řešení v celých číslech x_j pro $j = 1, 2, \ldots, n$ právě tehdy, je-li $\mathrm{NSD}(m_i, m_j) \mid (r_i - r_j)$ pro všechny indexy $i, j \leq n$. [11 s. 42]

Příklad 7.4 (Problém s košem vajec) Předpokládejme, že košík obsahuje *n* vajec. Bereme-li vejce z košíku po dvou, resp. 3, 4, 5, 6, pak v košíku zůstane 1, resp. 2, 3, 4, 5 vajec.

Řešení: Podle věty 7.3 můžeme zapsat rovnici

$$x = 2x_1 + 1 = 3x_2 + 2 = 4x_3 + 3 = 5x_4 + 4 = 6x_5 + 5 = 7x_6 .$$

Je jednoduché zkontrolovat, že podmínka NSD(m_i, m_j) | ($r_i - r_j$) platí pro všechny indexy $i, j \le 6$, kde $m_1 = 2, m_2 = 3, m_3 = 4, m_4 = 5, m_5 = 6, m_6 = 7$ a $r_1 = 1, r_2 = 2, r_3 = 3, r_4 = 4, r_5 = 5, r_6 = 0$. Podle věty 7.3 existuje řešení a tím nejmenším je x = 119.

Tento problém je připisován hindskému matematikovi Brahmaguptovi. Příklady 7.2 a 7.4 převzaty z [11 s. 41–43].

7.1 Modulární reprezentace

Věta 7.5 (Čínská zbytková věta) Mějme soustavu kongruencí

$$\begin{aligned} x &\equiv b_1 \pmod{m_1} \\ x &\equiv b_2 \pmod{m_2} \\ &\vdots \\ x &\equiv b_n \pmod{m_n}, \end{aligned}$$

kde pro každé $i \neq j$ platí NSD(m_i, m_j) = 1, tzn. že moduly jsou po dvou nesoudělné. Potom tato soustava má právě jedno řešení pro libovolné strany $b_1,\ldots,b_n$. Toto řešení je tvaru

$$x \equiv M_1 \overline{M_1} b_1 + M_2 \overline{M_2} b_2 + \ldots + M_n \overline{M_n} b_n \pmod{M},$$

kde $M = m_1 \cdot m_2 \cdot \ldots \cdot m_n$, $M_j = \frac{M}{m_j}$ a $\overline{M_j}$ je číslo, které vyhovuje $M_j \overline{M_j} \equiv 1 \pmod{m_j}$.

Příklad 7.6 Jsou dány rovnice

$$x \equiv 2 \,(\mathrm{mod}\, 5),\ x \equiv 3 \,(\mathrm{mod}\, 8),\ x \equiv 6 \,(\mathrm{mod}\, 11),\ x \equiv 4 \,(\mathrm{mod}\, 9)\,.$$

Řešení: NSD(5, 8, 11, 9) = 1 $\rightarrow$ soustava má právě jedno řešení.

Podle věty 7.5 spočítáme

$$M = 5 \cdot 8 \cdot 11 \cdot 9 = 3960$$

$$M_1 = 792,\ M_2 = 495,\ M_3 = 360,\ M_4 = 440$$

$$\overline{M_1} = 3,\ \overline{M_2} = 7,\ \overline{M_3} = 7,\ \overline{M_4} = 8\,.$$

Dosazením do rovnice

$$x \equiv 792 \cdot 3 \cdot 2 + 495 \cdot 7 \cdot 3 + 360 \cdot 7 \cdot 6 + 440 \cdot 8 \cdot 4 \ (\mathrm{mod}\, 3960)$$
$$x \equiv 44348 \ (\mathrm{mod}\, 3960)$$
$$x \equiv 787 \ (\mathrm{mod}\, 3960)$$

dostáváme řešení.

7.2 Historická poznámka

První podoby čínské věty o zbytcích se objevují počátkem třetího století (možná i dříve). Jednou z prvních úloh, která se objevila ve staré Číně, je nazývána *úloha o drůbeži*. Úloha zní: kolik kohoutů, slepic a kuřat je možné koupit za 100 mincí, jestliže zvířat je dohromady 100 a kohout stojí 5 mincí, slepice 4 mince a 4 kuřata stojí jednu minci? Postupem času přišli čínští matematici na několik řešení. Tato úloha se velmi rozšířila a získávala nové podoby. Další složitější úlohu, která v té době vznikla, je již uvedena na začátku této kapitoly. Autor úlohy **Sun Tsu**, též nazývaný **Sun-c'**, byl čínský matematik, který žil mezi třetím a pátým století našeho letopočtu (některé zdroje uvádějí první století). Je autorem díla *Suan Ťing*, kde se zabýval diofantickými rovnicemi. Toto jeho jediné známé dílo zmiňuje i čínskou zbytkovou větu. Vznik podobných úloh souvisel s astronomickými výpočty kalendáře. Úloha Sun-c' se také šířila dál. V různých obměnách se objevuje například v Indii nebo u **Fibonacciho**. V 15. století byla k nalezení v německých rukopisech, v 17. století pak v ruských. Staročínskou metodu rozpracoval také **Leonard Euler** a po něm **C. F. Gauss**.

8 Fibonacciho čísla

Fibonacciho posloupnost je nekonečná posloupnost čísel $\{0,1,1,2,3,5,8,13,21,\ldots\}$, kde každé číslo je součtem dvou předchozích a prvky posloupnosti se nazývají *Fibonacciho čísla*.

Rekurzivní definice Fibonacciho posloupnosti je

$$F_n = \begin{cases} 0, & \text{pro } n = 0 \\ 1, & \text{pro } n = 1 \\ F_{n-1} + F_{n-2}, & \text{jinak} \end{cases}.$$

Jak uvádí Donald Knuth v knize [5 s. 80], první zmínky o spojitosti Fibonacciho čísel a Euklidova algoritmu se objevily roku 1837, kdy É. Léger využil posloupnost čísel F_n ke studiu efektivity algoritmu. V 70. letech 19. století získal É. Lucas velmi přesné výsledky o Fibonacciho číslech.

Věta 8.1 (Lucas) Číslo dělí F_m a F_n, právě když je dělitelem F_d, kde $d = \text{NSD}(m, n)$; zejména,

$$\text{NSD}(F_m, F_n) = \text{F}_{\text{NSD}(m, n)}.$$

Důkaz: Tento výsledek dokážeme pomocí Euklidova algoritmu. Vidíme, že vzhledem k

$$F_{n+m} = F_m F_{n+1} + F_{m-1} F_n$$

je každý společný dělitel F_m a F_n také dělitelem F_{n+m}, a naopak, každý společný dělitel F_{n+m} a F_n je také dělitelem $\text{F}_m F_{n+1}$. Protože F_{n+1} je s F_n nesoudělné, společný dělitel F_{n+m} a F_n dělí také F_m. Dokázali jsme tudíž, že pro libovolné číslo d platí:

d dělí F_m a F_n, právě když d dělí $\{F_{m+n}, F_n\}$.

Nyní ukážeme, že každá posloupnost $\{F_n\}$, pro kterou platí předchozí tvrzení a pro kterou je $F_0 = 0$, splňuje také větu 8.1.

Předchozí výrok můžeme indukcí podle k rozšířit do tvaru

d dělí F_m a F_n, právě když d dělí $\{F_{m+kn}, F_n\}$,

kde k je libovolné nezáporné celé číslo. Tento výsledek můžeme formulovat stručněji:

d dělí $F_{m \pmod n}$ a F_n, právě když d dělí $\{F_m, F_n\}$.

Jestliže nyní r je zbytek po dělení m číslem n, tedy jestliže $r \equiv m \pmod n$, pak každý společný dělitel $\{F_m, F_n\}$ je také společným dělitelem $\{F_n, F_r\}$. Z toho vyplívá, že při manipulaci v Euklidově algoritmu zůstává množina společných dělitelů $\{F_m, F_n\}$ nezměněna i při měnícím se m a n; konečně pokud je $r = 0$, jsou společní dělitelé jednoduše děliteli $F_0 = 0$ a $F_{NSD(m, n)}$.

Převzato z [5 s. 81]. □

Při analýze počtu kroků dělení Euklidova algoritmu jsou dvě po sobě jdoucí Fibonacciho čísla jako vstupní hodnoty nejhorší variantou.

Příklad 8.2 Mějme 2 přirozená čísla a, b, pro která Euklidův algoritmus vyžaduje právě 5 kroků. Jak velké bude b?

Řešení: Napíšeme si Euklidův algoritmus v pěti krocích.

$$\begin{aligned} a &= q_1 b + r_1 & 0 \le r_1 < b \\ b &= q_2 r_1 + r_2 & 0 \le r_2 < r_1 \\ r_1 &= q_3 r_2 + r_3 & 0 \le r_3 < r_2 \\ r_2 &= q_4 r_3 + r_4 & 0 \le r_4 < r_3 \\ r_3 &= q_5 r_4 + 0 \end{aligned}$$

Nejdříve si všimněme, že r_4 musí být různé od 0 (protože algoritmus má pět kroků), a tedy

$$r_4 \ge 1.$$

Dále platí $r_4 < r_3$ a z toho plyne

$$r_3 \ge 2.$$

Jak velké bude r_2 ? Ze čtvrté rovnice $r_2 = q_4 r_3 + r_4$ plyne, že $r_2 \ge r_3 + r_4$ a po dosazení dostaneme $r_2 \ge 2 + 1$, takže

$$r_2 \ge 3.$$

Stejným způsobem zjistíme, že $r_1 \ge 3 + 2$ a tím pádem je

$$r_1 \geq 5 .$$

Nakonec opět stejným způsobem získáme b z nerovnosti $b \geq r_1 + r_2$ a z toho dostáváme

$$b \geq 8 .$$

Možná je již patrné, že čísla v nerovnicích tvoří posloupnost Fibonacciho čísel.

Závěr: Jestliže má Euklidův algoritmus čísel *a*, *b* pět kroků, pak $b \geq F_6$. Můžeme to říct i obráceně: jestliže $b < F_6$, pak bude mít algoritmus nejvíce 4 kroky.
Výsledek tohoto příkladu je dále vyjádřen obecně.
Převzato z [20 s. 163–164].

Věta 8.3 Nechť *a*, *b*, $n \in \mathbb{N}$. Jestliže $b < F_{n+2}$, pak Euklidův algoritmus provedený na číslech *a*, *b* bude mít nejvíce *n* kroků. [20 s. 164]

Pokud je ještě navíc $a = F_{n+2}$ a $b = F_{n+1}$ (pro každé $n \geq 0$) pak má algoritmus právě *n* kroků.

Věta 8.4 (Lamé) Pro $n \geq 1$, nechť *u* a *v* jsou celá čísla, přičemž $u > v > 0$, taková, že Euklidův algoritmus nad *u* a *v* vyžaduje právě *n* kroků dělení a že *u* je co nejmenší z čísel splňujících tyto podmínky. Potom je $u = F_{n+2}$ a $v = F_{n+1}$. [7 s. 360]

Věta 8.3 platí pro $b \leq 100$, první Fibonacciho číslo větší než 100 je $F_{12} = 144$, takže pro $b < F_{12}$ věta zaručuje, že Euklidův algoritmus bude mít nejvíce 10 kroků.

Fibonacciho čísla můžou být aproximována mocninou zlatého řezu[12] ϕ. Platí

$$\phi^n < F_{n+2} .$$

Pokud chceme nalézt Fibonacciho číslo větší než 100, stačí najít takové číslo $n \in \mathbb{N}$, pro které

$$100 \leq \phi^n .$$

Zlogaritmováním obou stran nerovnice dostaneme *n*:

$$n \geq \log_\phi 100 .$$

[12] více v historické poznámce 8.1

Věta 8.5 Nechť $a, b \in \mathbb{N}$ a $b > 1$. Potom počet kroků potřebných na provedení Euklidova algoritmu čísel a, b je nanejvýš

$$\lceil \log_\phi b \rceil,$$

kde $\lceil ... \rceil$ značí horní celou část[13] čísla $\log_\phi b$.

Převzato z [20 s. 166–167].

Příklad 8.6 Spočítejte počet kroků Euklidova algoritmu čísel a, b.

$$a = 951831421, \quad b = 616457820$$

Řešení: Nejdříve spočítáme[14]

$$\log_\phi b = 42{,}0546...$$

Horní celá část tohoto čísla je tedy

$$\lceil 42{,}0546... \rceil = 43.$$

Závěr: Euklidův algoritmus bude mít v tomto případě nejvýše 43 kroků.

[13] jestliže $x \in \mathbb{R}$, tak $\lfloor x \rfloor$ je největší celé číslo větší nebo rovné x

[14] nejlépe zadáním do nějakého matematického programu, například WolframAlpha nebo Matlab

8.1 Historická poznámka

Fibonacciho posloupnost poprvé popsal italský matematik **Leonardo Pisano**, též nazývaný **Fibonacci** (cca 1175–1250). Touto posloupností popisoval poněkud zidealizovaný růst populace králíků, protože králíci zde neumírají, nejsou nemocní a vždy zplodí pár, který je schopen reprodukce od druhého měsíce života, a pak každý další měsíc zplodí nový pár. Tedy první měsíc ($n = 1$) máme jeden pár, tzn. $F_1 = 1$, druhý měsíc ($n = 2$) máme stále jeden pár, $F_2 = 1$. Třetí měsíc ($n = 3$) zplodí nový pár, $F_3 = 2$. Čtvrtý měsíc ($n = 4$) zplodí původní pár nový pár a k tomu máme pár narozený minulý měsíc, tudíž $F_4 = 3$. Pátý měsíc bude párů již 5. Takto bychom mohli počítat do nekonečna za předpokladu, že jsou králíci nesmrtelní. Počet párů za každý měsíc nám tedy dá posloupnost $\{1,1,2,3,5,8,13,21,\ldots\}$.

Fibonacci se narodil v Itálii v Pise, jeho otec byl obchodník a vysoký úředník. Později se stal konzulem v nové pisánské kolonii, v dnešním Alžíru. Leonardo tam odjel s ním a seznámil se tam s arabskými číslicemi. Později s podporou otce procestoval celé Středomoří, kde se učil matematiku od nejlepších učenců tehdejší doby. Jeho nejslavnější knihou je *Liber abaci* (v překladu kniha o abaku[15]), dalším spisem, který vydal, je sbírka řešených příkladů s názvem *Flos*. Ta dokonce zaujala císaře Fridricha II., kterého bavila matematika a s Fibonaccim se přátelil. Fibonacci je považován za nejvýznamnějšího matematika středověké Evropy.

Fibonaccimu je připisováno pokračování příběhu zlatého řezu:
„Zlatý řez byl výrazem řecké touhy po přirozené harmonii věcí a tvarů. O něco matematičtěji řečeno, byl to úkol najít poměr dvou čísel, řekněme a a b, tak, aby větší bylo ve stejném poměru k menšímu, jako součet obou k většímu. S použitím vzorců to vypadá srozumitelněji, chtěli, aby

$$a : b = (a + b) : a .$$

[15]abak byl výpočetní přístroj starověku a středověku, kniha *Liber abaci* však není o počítání na abaku, ale o početních metodách

Staří Řekové si všimli, že dělení na dva stejné díly nepůsobí ani zdaleka tak hezky, jako když je jeden kousek o trochu delší. Problém vede po úpravě na kvadratickou rovnici

$$c^2 + c = 1,$$

která neurážela jejich nechuť k záporným číslům a kde c byl hledaný poměr a/b.“ [16 s. 80]

Řešením (pouze kladným) je

$$c = \frac{\sqrt{5}-1}{2} \cong 0{,}618033989,$$

tedy zlatým řezem je nazván poměr

$$1 : 0{,}618.$$

Pro Fibonacciho posloupnost

$$1, 2, 3, 5, 8, 13, 21, 34, 55, 89,\ldots$$

platí, že podíly každého čísla s následujícím jsou

$$1; 0{,}5; 0{,}666\ldots; 0{,}6; 0{,}625; 0{,}615\ldots; 0{,}619\ldots\ 0{,}6176\ldots; 0{,}61818\ldots$$

Je vidět, že se podíly stále více přibližují zlatému řezu až s ním po nekonečně mnoha krocích splyne. Zlatý řez se většinou označuje ϕ.

9 Programování

V dnešní době počítačů lze samozřejmě Euklidův algoritmus zapsat do počítačového programu a ten za nás vypočítá výsledek. Podle potřeby lze zadání programu různě modifikovat nebo rozšiřovat. Základní algoritmus není složitý, proto jsem ho pro ilustraci naprogramovala, viz příloha 1 a 2. Vybrala jsem si programovací jazyk Pascal, se kterým jsme pracovali v prvním ročníku.

Nejdříve musíme vytvořit zdrojový kód programu, což znamená, že algoritmus zapíšeme v programovacím jazyku. V Pascalu (jako i v jiných) je potřeba nejdříve nadefinovat proměnné a jejich typ, to se nazývá deklarace proměnných (zkratka *var*). V našem případě máme proměnné *x*, *y* a datový typ *longint*, ten řadíme do jednoduchých celočíselných typů. Pak už můžeme začít psát samotný program, tedy přejdeme k příkazové části. Nadefinujeme Euklidův algoritmus s použitím funkce modulo. Pak už jen programu nařídíme, co vše má při spuštění vypisovat. Po spuštění nám soubor umožní zadat proměnnou *x*, stisknutím klávesy *enter* můžeme zadat proměnnou *y* a po dalším stisknutí enteru nám program vypíše výsledek, tedy největšího společného dělitele čísel *x* a *y*. Vše právě popsané je k dispozici v přílohách 1 a 2.

Při testování programu jsem ovšem narazila na problém. Můj program funguje dobře, ale ne pro dvě velká čísla (např. 1576468 a 333333). Pro běžné používání je program dostačující, ovšem pro použití velkých čísel bylo potřeba program upravit. Převážně s pomocí svého kamaráda jsem program upravila tak, aby vyhovoval požadavku na velká čísla. Úpravy programy byly následující:

- ve všech funkcích a proměnných je použitý typ Int64 (větší rozsah čísel)
- vypnutí Range Checkingu (testování rozsahu čísel) direktivou {$R-}
- vstupy hodnot se nyní z řetězců převádějí až po zadání, takže lze otestovat vstupní data, zda nebyly zadány nesmysly.

Tím jsem získala druhý program, který by měl pokrýt opravdu velký rozsah čísel. Tento program je k prohlednutí v přílohách 3 a 4.

Závěr

Tato práce by měla představovat ucelený text o základech Euklidova algoritmu. Cílem bylo sepsat několik kapitol o pojmech spojených s Euklidovým algoritmem, vše vysvětlit a přidat něco z historie. Jedním z důvodů, proč jsem chtěla vytvořit příručku základních pojmů souvisejících s Euklidovým algoritmem, bylo to, že v češtině je něco takového těžko k sehnání. Poznala jsem to sama při sbírání materiálu, převážně jsem informace čerpala z anglických textů, z nichž jsem postupně skládala vyjmuté části dohromady. Nedostatek českých publikací je problém nejen Euklidova algoritmu, ale i jiných matematických pojmů. Práce s anglickým textem je i pro pokročilejší angličtináře někdy obtížná na pochopení obsahu, a tím časově náročnější.

Pro shrnutí řekněme, že Euklidův algoritmus byl a je jedním z nejpoužívanějších algoritmů, má široké využití, především souvisí s určením největšího společného dělitele a to nejen pro přirozená čísla, ale dále například pro polynomy. Jeho rozšířením pro Bézoutovu rovnost obdržíme koeficienty jeho lineární kombinace. Aplikací algoritmu můžeme získat i inverzní prvek, ten se v současnosti využívá v šifrování a kódování. Euklidův algoritmus také souvisí s Fibonacciho čísly.

Na závěr bych chtěla podotknout, že bakalářská práce byla přínosem především pro mě samotnou. Za dobu strávenou tvorbou bakalářské práce jsem se naučila rozebrat odborný text, zlepšila schopnost pracovat s textovým editorem, procvičila jsem si anglický jazyk a hlavně jsem si rozšířila znalosti a dozvěděla se spoustu nových poznatků, i těch, co s tématem této práce nesouvisely.

Seznam použitých zdrojů a literatury

[1] *WIKIPEDIA – The Free Encyclopedia* [online]. [vid. 2012-09-03]. Dostupné z: http://en.wikipedia.org/wiki/Euclidean_algorithm

[2] BURTON, David M., *Elementary Number Theory*. 6. vydání. Boston: McGraw-Hill Higher Education, 2007. ISBN 978-0-07-305188-8.

[3] CHABERT, Jean-Luc. *A History of Algorithms: From the Pebble to the Microchip*. 1. vydání. Berlin: Springer, 1999. ISBN 3-540-63369-3.

[4] EUKLEIDES. *Základy*, *Knihy VII-IX*. 1. vydání. Kanina: OPS, 2010. ISBN 978-80-87269-11-4.

[5] KNUTH, Donald E., *Umění programování, 1. díl Základní algoritmy*. 1. vydání. Brno: Computer Press, 2008. ISBN 978-80-251-2025-5.

[6] SCHEID, Von Harald. *Elemente der Arithmetik und Algebra*. 2. přepracované vydání. Mannheim: Bibliographisches Institut & F.A. Brockhaus AG, 1992. ISBN 3-411-14922-1.

[7] KNUTH, Donald E., *Umění programování, 2. díl Seminumerické algoritmy*. 1. vydání. Brno: Computer Press, 2010. ISBN 978-80-251-2898-5.

[8] STANOVSKÝ, David. *Základy algebry*. 1. vydání. Praha: Matfyzpress, 2010. ISBN 978-80-7378-105-7.

[9] NOVOTNÁ, J., TRCH, M., *Algebra a teoretická aritmetika, Sbírka příkladů, 2.část – Polynomická algebra*. 2. doplněné vydání. Praha: Univerzita Karlova v Praze – Pedagogická fakulta, 2000. ISBN 80-7290-007-2.

[10] *WIKIPEDIE – Otevřená encyklopedie* [online]. [vid. 2012-11-18]. Dostupné z: http://cs.wikipedia.org/wiki/Fibonacciho_posloupnost

[11] MOLLIN, Richard A., *Fundamental Number Theory with Applications*. 2. vydání. Boca Raton: Chapman, 2008. ISBN 978-1-4200-6659-3.

[12] LAURITZEN, Niels. *Concrete Abstract Algebra: From Numbers to Gröbner Bases*. 1. vydání. New York: Cambridge University Press, 2003. ISBN 05-215-3410-0.

[13] SILVERMAN, Joseph H., *A Friendly Introduction to Number Theory*, 4. vydání. Boston: Pearson, 2012. ISBN 978-03-218-1619-6.

[14] HARDY, D.W., RICHMAN, F., WALKER, C. L., *Applied Algebra: Codes, Ciphers and Discrete Algorithms*. 2. vydání. Boca Raton: CRC Press, 2009. ISBN 978-1-4200-7142-9.

[15] BEČVÁŘ, J., FUCHS, E., *Historie matematiky I*: *Seminář pro vyučující na středních školách*. Brno: Jednota českých matematiků a fyziků, 1994.

[16] MAREŠ, Milan. *Příběhy matematiky: stručná historie královny věd*. 2. revidované vydání. Příbram: Pistorius, 2011. ISBN 978-808-7053-645.

[17] VÍT, Pavel. *Řetězové zlomky*. 1. vydání. Praha: Mladá fronta, 1982.

[18] JUŠKEVIČ, Adolf P., *Dějiny matematiky ve středověku*. 1. vydání. Praha: Academia, 1978.

[19] *WIKIPEDIA – The Free Encyclopedia* [online]. [vid. 2012-03-06]. Dostupné z: http://en.wikipedia.org/wiki/Polynomial

[20] POMMERSHEIM, J., MARKS, T., FLAPAN, E., *Number Theory: A Lively Introduction with Proofs, Applications, and Stories*. 1. vydání. Hoboken: Wiley, 2010. ISBN 978-047-0424-131.

[21] VILD, Jaroslav. *Přednášky: Algebra a geometrie 1, 2; Algebra a aritmetika*.

[22] KOUCKÝ, Miroslav. *Přednášky: Úvod do diskrétní matematiky*.

[23] MLÝNEK, Jaroslav. *Přednášky: Kryptografie a bezpečnost informací*.

[24] OLEHLA, Milan. *Počítače a programování - PASCAL*. 4. vydání. Liberec: TUL, 2010. ISBN 978-80-7372-603-4.

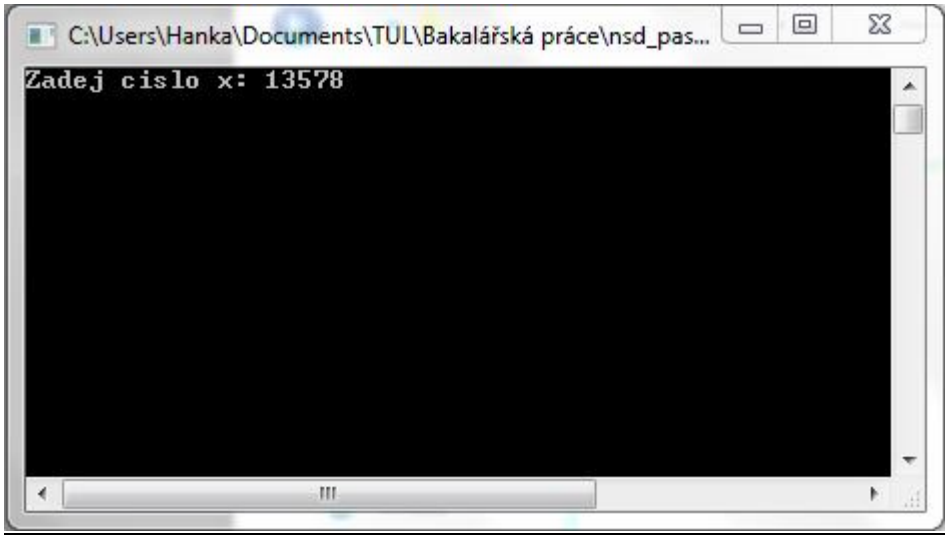
Seznam příloh

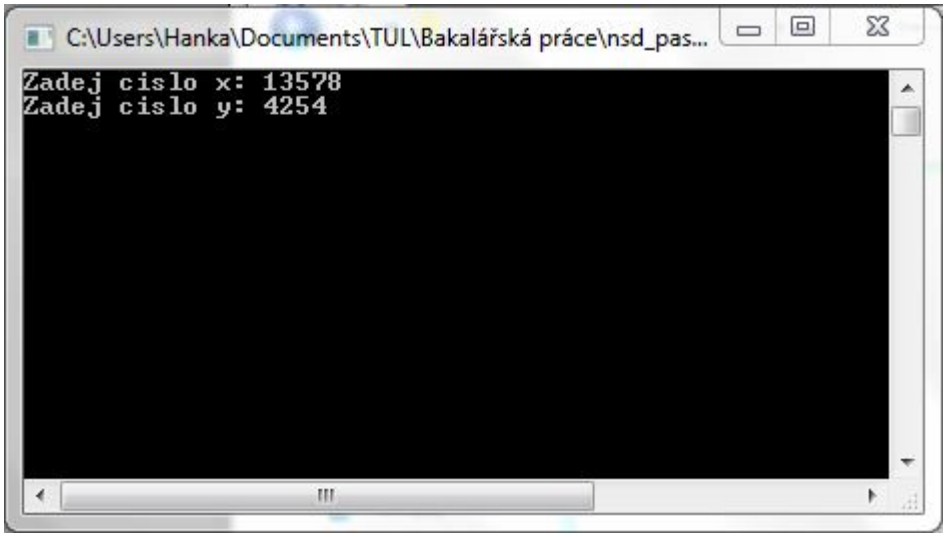
Přílohy k bakalářské práci

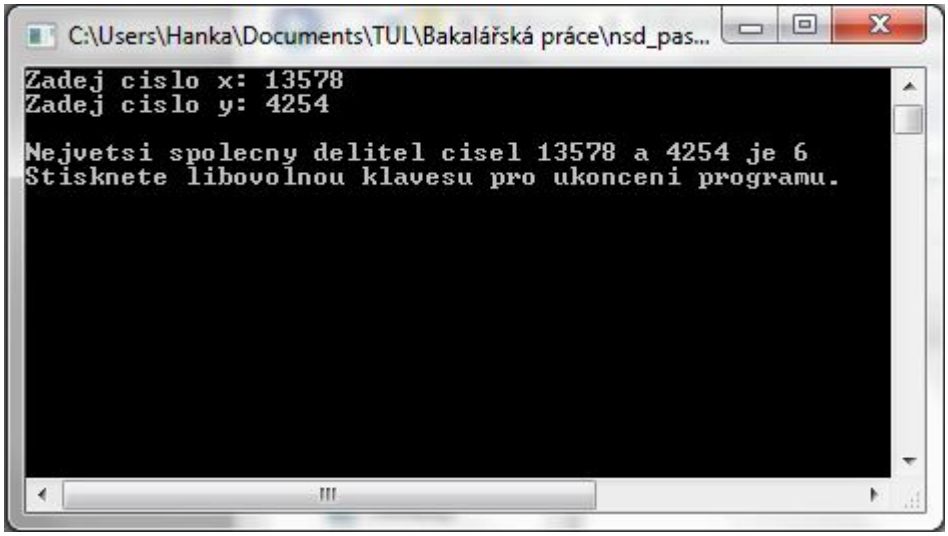
Příloha 1: Euklidův algoritmus pro výpočet největšího společného dělitele
(počítačový program 1)

```
program NSD;
{$APPTYPE CONSOLE}
uses SysUtils;
var x,y:longint;

function nsd(a,b:longint):longint; // nejvetsi spolecny delitel
var
  zbytek:integer;
begin
  repeat // opakujeme dokud zbytek deleni neni nula
    zbytek:=a mod b; // modulo a,b (zbytek po deleni)
    a:=b;
    if zbytek = 0 then break else b:=zbytek;
  until zbytek=0;
  nsd:=b;
end;

begin

  // zadani vstupnich hodnot
  write('Zadej cislo x: ');
  readln(x);

  write('Zadej cislo y: ');
  readln(y);

  writeln;

  // volani funkce s navratovou hodnotou vysledku
  writeln('Nejvetsi spolecny delitel cisel ',x,' a ',y,' je ', nsd(x,y));

  // cekani na libovolnou klavesu
  writeln('Stisknete libovolnou klavesu pro ukonceni programu.');
  readln;

end.
```

Příloha 2: Příklad spuštěného programu 1







Příloha 3: Euklidův algoritmus pro výpočet největšího společného dělitele
(počítačový program 2)

```
program NSD;
{$APPTYPE CONSOLE}
{$R-}
uses SysUtils;
var x,y:Int64;
    xstr,ystr : String;

// vraci zbytek po deleni vetsiho cisla mensim
function Modulo(a,b:Int64):Int64;
var
 vysl,c : Int64;

begin
 if (a<b) then
  begin
   c:=a;
   a:=b;
   b:=c;
  end;
 vysl:=Trunc(a/b);
 Modulo:=a-(vysl*b);
end;

// vraci nejvetsiho spolecneho delitele
function NSD(a,b:Int64):Int64;
var
  zbytek:integer;
begin
  repeat // opakujeme dokud zbytek deleni neni nula
    zbytek:=Modulo(a,b);
    a:=b;
    if zbytek = 0 then break else b:=zbytek;
  until zbytek=0;
  nsd:=b;
end;


begin
  writeln('NSD - nejvetsi spolecny delitel');
  writeln('vstupni hodnoty cisel mohou byt v rozsahu 1 az
  9223372036854775807');
  writeln;
```

```
 // zadani vstupnich hodnot
  write('Zadej cislo x: ');
  readln(xstr);
  write('Zadej cislo y: ');
  readln(ystr);
  writeln;

  // prevod retezcu na Int64
  x:=StrToInt64Def(xstr,-1);
  y:=StrToInt64Def(ystr,-1);

  // pokud doslo k spravnemu prevodu na cisla volame funkci NS
  if (x>1) and (y>1) then
   begin
    writeln('Nejvetsi spolecny delitel cisel ',x,' a ',y,' je ', NSD(x,y),'.');
   end else writeln ('Chyba ve vstupnich udajich.');

  // cekani na libovolnou klavesu
  writeln;
  writeln('Stisknete libovolnou klavesu pro ukonceni programu.');
  readln;

end.
```

Příloha 4: Příklad spuštěného programu 2